2001

TRANSLATION OF HOMEWORK BY OBLTN. W. WERTHER, COMPANY COMMANDER OF 7/LN.Rgt. 353, written on 12 August 1945 at ADI(K)

The attached report covers PW's account of the following subjects:-

a. Codes and Ciphers of the Soviet Air Force 1937-45 and their treatment by the cryptanalytic service of the GAF.

b. The separate elements of Soviet cipher systems.

c. Cipher system of the Soviet Air Force 1937-1945 and the successes of GAF cryptanalysis in general.

d. Modus operandi of GAF cryptanalysis in dealing with Soviet Air Force systems.

e. Examples of Soviet Air Force cipher systems in use during the campaign in the East.

f. Principles of the Soviet call-sign system.

TICOM
3 Oct. 45

Copy No. 23
No. of pages 69

DISTRIBUTION.

British

1 D.D.3
2 H.C.G.
3 D.D. (N.S.)
4 D.D. (M.W.)
5 D.D. (A.S.)
6 C.C.R.
7 Lt. Col. Leatham
8 Cdr. Tandy
9 Major Morgan

U.S.

10-11 p-20-G (2) (via Lt.Cdr. Manson)
12 G-2 (via Lt.Col. Hilles)
13-15 A.S.A. (3) (via Major Seaman)
16 Director, S.I.D. USFET (via Lt.Col. Johnson)
17 Col. Lewis Powell, USSTAF.

TICOM

18 Chairman
19-21 S.A.C. (3)
22 Cdr. Bason
23 Lt.Col. Johnson
24 Major Seaman
25 Lt.Cdr. Manson
26 Major Cowan
27 Lt. Fehl
28-31 Ticom Files (4)

Additional

32-34 Lt. Col. Pritchard (3)

Approved for Release by NSA on 07-25-2017, FOIA Case # {66109}

DO NOT Distribute to the NSA Technical Library when no longer needed
S-4752 Acc. No. 2

Doc ID: 6587327

THE CODES AND CIPHERS OF THE SOVIET AIR FORCE, 1937 - 1945, AND THEIR TREATMENT BY THE CRYPTOGRAPHIC SERVICE OF THE G. A. F.

Contents

page

7 Foreword

I. CHARACTERISTICS COMMON TO ALL SOVIET CIPHER SYSTEMS

8 II. INDIVIDUAL TYPES OF SOVIET CIPHER SYSTEMS

A. Basic Types of Cipher

1. Substitution

a. Simple substitution
9 b. Multiple substitution
10 c. Expanded substitution ((erweiterter Caesar))

2. The table

11 3. The code table
12 Example of an air to ground coding card (reconnaissance)

13 4. The basic book

a. Relative arrangement of the various code-book significations

aa. The non-hatted basic book
bb. The partly hatted basic book
14 cc. The hatted basic book

b. Enciphering of figures

aa. Basic book without figure significations
15 bb. Basic book with non-hatted figure significations
cc. Basic book with partly hatted figure significations
16 dd. Basic book with hatted figure significations

c. Internal structure

17 aa. Basic book without special sections
bb. Basic book with special sections

d. Structure of the different basic book significations

aa. Book groups with one signification
bb. Book groups with several significations

18 e. Common groups

aa. One group for each signification
bb. Alternative groups for each signification

Doc ID: 6587327

Page

19 5. Seperate code tables.

a. Coding table for addresses ((i.e. delivery groups))
20 b. Coding table for A/C types

6. Proformas

21 7. Lettered coordinates

8. Meteorological ciphers

22 B. Reciphering methods

1. Reciphering keys

a, Arrangement of individual elements of reciphering keys

aa. The non-hatted key
23 bb. The partly hatted key
cc. The hatted key

b. Variants of the same keys

aa. Different keys derived from one series of figures
24 bb. "Magic Squares" /(Trommelvariationen)
cc. Independent keys

c. Values of individual elements of a key

aa. Keys with one equivalent for each element
bb. Keys with several equivalents for each element

25 d. Comparison of different kinds of recipher keys

aa. Trommelvariationen (see B. 1. b. aa. above)
bb. Keys obtained from "magic squares"
cc. Independent keys

2. Substitution tables

26 3. Addey tables

a. Addeys used more than once
27 b. Addeys used once only

28 C. Reciphering

1. Reciphering system

a. The process of reciphering

aa. Simple reciphering
29 bb. Multiple reciphering

b. Series of recipher keys

Doc ID: 6587327

page

30 2. Change of reciphering tables

a. Infrequent change of reciphering tables.
b. Frequent (individual) change of reciphering tables.
c. Change of figure values in the reciphering system.
d. Change of reciphering system.

31 3. The key group (the indicator)

a. The indicator in the cipher message.
b. Method of reading the indicator.
32 c. Composition of the indicator.

33 4. The dummy.

5. Method of reading the cipher group (the indicator).

III THE CIPHERS OF THE SOVIET AIR FORCE 1937-45 AND THE SUCCESSES OF GAF CRYPTOGRAPHY IN GENERAL.

34 A. 1937-39.

1. Practice messages.

a. Nonsense practice messages.
b. Tactical practice messages.

2. The two-figure table in general use.

35 3. The three-figure Air Force code in general use.

a. The 1937-38 three-figure Air Force code-book.
b. The 1939 three-figure Air Force code-book("WAK-39")
c. The 1940 (?) Air Force code-book.

36 4. The four-figure staff system in general use, so-called "Commanders' Code".

a. The 1937 four-figure system (called "Privo").
37 b. The 1938-39 four-figure system ("okk-5").

38 5. The five-figure adder in general use.

6. Proformas.

7. Primitive ciphers.

B. The occupation of Eastern POLAND by the Red Army in September 1939.

C. The winter campaign in FINLAND, 1939-40.

39 1. Two and three-figure messages.
2. "Okk 5" messages.
3. The five-figure system.

40 D. Reorganisation of SOVIET cipher systems on the basis of experiences in the winter campaign in FINLAND.

Doc ID: 6587327

Page

1. Abolition of most general systems - institution of regional systems.
41 2. Shortening of the period of validity of the systems.
3. Complication of the cipher instructions.
4. Complication of the reciphering systems.
5. Ousting of non-batted systems.
42 6. Shortening of the period of validity of recipher keys, introduction of "individual" recipher keys.
7. Introduction of dummies.
8. Abolition of the two-figure tables in general use for wireless operators.
9. Complication of the retained five-figure adder in general use.
10. The use of machine ciphers.
43 11. Introduction of transposition systems?

IV THE MODUS OPERANDI OF GAF CRYPTOGRAPHY IN DEALING WITH SOVIET AIR FORCE SYSTEMS.

A. Breaking a new cipher.

1. Analysis of the message.

a. The statistical picture.
44 b. Normal statistical picture.
aa. Normal two-figure statistical picture.
bb. Normal three-figure statistical picture.
cc. Normal four-figure statistical picture.
45 2. Reduction of the normal statistical picture
3. Stripping of reciphers.
4. Breaking into the system.

46 Example of a normal three-figure statistical picture.
47 Example of a normal four-figure statistical picture.
48 Reduction of the normal statistical picture on p.
49 Second normal four-figure statistical picture.
50 Reduction of the normal statistical picture on p. and reduction of the statistical picture on p.

51 5. Breaking into the cipher text.
6. New interpretation of items, decoding.
7. Recovery of original basic book.
8. Recovering the reciphering system.
9. Working out the system.
52 10. Naming the systems which have been solved.

53 B. Breaking the five-figure adders.

1. Determining the indicators (starting points).
2. Writing messages one below the other.
3. Compiling the catalogue of differences.
54 4. Relating different columns to each other.
55 5. Frequency statistics.

Doc ID: 6587327

page

55 6. Decoding.

7. Recovery of original cypher instructions.

C. Deciphering.

1. Cipher recognition service.

a. Call-sign or network identification
b. Message groups.
56 c. Key groups (indicators).
d. Address groups.
e. General message characteristics
f. Statistical picture.

2. Recipher investigations.

a. Contents of the message
57 b. The reciphering system.
c. The basic code.

3. Interpretation of new items.

D. Aids to cryptography.

1. General aids and data.

2. Special aids and data.
a. Letter and figure counts.
b. Language statistics.
58 c. Special indexes.
d. Message files.

V. EXAMPLES OF SOVIET AIR FORCE CIPHER SYSTEMS IN USE DURING THE CAMPAIGN IN THE EAST.

1. The PT-table.
Reconstructed PT-tables.

60 2. Key tables with 200 positions.
Reconstruction of the table.

62 3. Cipher table of a flying unit.
Reconstruction of the table.

64 4. 10-page basic book of the general organisation.
Reconstruction of the basic book and of the reciphering system.

66 5. 10-page basic book of the ground organisation.
Reconstruction of the basic book.
Reconstruction of the reciphering system.

APPENDIX

70 1. Organisation of CHI-STELLE East.

2. Principles of the SOVIET call-sign system.

3. The Forschungsamt.

Doc ID: 6587327

THE CODES AND CIPHERS OF THE SOVIET AIR FORCE, 1937-1945, AND THEIR TREATMENT BY THE CRYPTOGRAPHIC SERVICE OF THE G.A.F.

FOREWORD

An attempt is made in this paper to depict in its main outlines the general behaviour of ciphers used by the Soviet Air Force before and during the war against GERMANY.

The difficulties which beset such an attempt at reconstruction are evident if it is remembered that the GAF cryptographic service on the Eastern Front had to deal every day with about 100 major cipher systems and that these were on the average chaged every three to four months. The cryptographic service of the GAF worked out more than 900 major cipher systems during the war against the SOVIET UNION, quite apart from unnumbered or elementary ciphers (and ciphers whose existence was not indicated on wireless networks) whose numbers run into thousands.

The author has personally worked on a large proportion of these systems or else supervised the work and advised others in a technical capacity, but he is not able to furnish more exact details, since no reference data were available while this paper was being written. The generally high volume of traffic intercepted and its great variety made it imperative for the sake of "mental hygiene" quickly to forget all details not essential to the daily task. This was particularly the case since a comprehensive filing system enabled every detail and every process to be reconstructed at any time.

This paper deals only with the systems of the SOVIET Air Force, but what is written here is conditionally valid for all the Armed Forces of the SOVIET UNION.

I. CHARACTERISTICS COMMON TO ALL SOVIED CIPHER SYSTEMS.

The general characteristics of SOVIET cipher systems can be summarised in the following points:

1. Substitution systems are used almost exclusively. The cipher text appears as a group of figures, thus the SOVIET wireless operator is accustomed only to send and recieve figure symbols. The chief kinds are substitution and code-book or table ciphers. These methods are varied in a number of ways and adapted in every case to their particular purpose.

2. The marked tendency to adhere to non-hatted construction is a notable feature, both in the provision of cipher data and in the use of reciphering methods. This fact was often of considerable assistance to cryptographic efforts.

3. The SOVIET encipherer knows no hard and fast universal basic rules, either in the set-up and form of the text to be enciphered (e.g. use of punctuation, rules for dealing with addresses and signatures etc) or in the application of the various fundamentals of enciphering. This lack of consistency in enciphering to some extent increases the difficulty of the work; every method has peculiarities which must be discovered anew in each case and which can in no case be taken for granted.

4. Very great importance is universally attached to secret transmission of signals. Even signals sent by land line (telephone conversations) are in principle to be enciphered. The instructions in most captured keys make special provision for this. On numerous

Doc ID: 6587327

occasions during the war, draconic punishments were ordered against signals personnel who infringed this rule, but the number of messages transmitted in clear, for instance, was nevertheless fairly considerable. There was apparently no systematic monitoring of their own wireless stations.

5. The maintenance of secrecy concerning their own cipher organisation is extraordinarily thorough. Enciphering and the deciphering of wireless and telephone messages was entrusted exclusively to specially selected and trained officers who were politically reliable. Since neither the men nor their officers had even the slightest knowledge of their own cipher service, the circle of those initiated remained amazingly small. For this reason it is almost impossible to assist the task of the cryptographers in technical matters by interrogating prisoners or by the Abwehr. On the other hand it is perfectly comprehensible from a psychological aspect that the troops were inclined to underestimate their own ciphering methods and means and thereby led to commit indiscretions.

II. THE SEPARATE ELEMENTS OF SOVIET CIPHER SYSTEMS.

A. THE KEY DATA.

Preliminary remark: The Russian alphabet is expressed in machine type as follows:-

a-	А	b-	Б	w-	В
g-	Г	d-	Д	e-	Е
v-	Ж	z-	З	i-	И
j-	Й	k-	К	l-	Л
m-	М	n-	Н	o-	О
p-	П	r-	Р	s-	С
t-	Т	u-	У	f-	Ф
h-	Х	c-	Ц	ß-	Ч
ch-	Ш	q-	Щ	y-	Ы
x-	Ъ	j-	Э	ü	Ю
g	Я				

1. Substitution.

a. Simple Substitution

Simple substitution is the simplest form of substitution cipher. Every letter has only one figure value in cipher. The statistics of a cipher text therefore yield both the number of letters used and their true frequency.

The security of the cipher is very low; in the case of non-hatted substitutions it sinks to nil.

EXAMPLE OF NON HATTED SUBSTITUTION:

→	0	1	2	3	4	5	6	7	8	9
0	а	б	в	г	д	е	ж	з	и	й
2	к	л	м	н	о	п	р	с	т	у
4	ф	х	ч	ц	ш	щ	ъ	ь	э	ю
6	я									

Doc ID: 6587327

EXAMPLE OF HATTED SUBSTITUTION

A - 29	I - 85	R - 12	CH - 77
B - 90	J - 30	S - 75	Q - 87
W - 63	K - 15	T - 57	Y - 41
G - 07	L - 70	U - 36	X - 78
D - 83	M - 42	F - 20	Ä - 14
E - 43	N - 03	H - 99	Ö - 97
V - 64	O - 94	C - 24	Ü - 52
Z - 16	P - 80	B - 48	

b. Multiple-Substitution Table

In the case of a multiple substitution table, individual letters - and particularly such as recur frequently, are each expressed by several code figures. This blurs the statistical picture to a greater or lesser degree. Compared with simple substitution, the security of the cipher is indeed higher, but the various equivalents can be reduced to a common denominator with the aid of parallel passages enciphered in different ways (addresses, commonly occurring word stems etc.) or by bigram statistics.

EXAMPLE OF NON HATTED SUBSTITUTION WITH SEVERAL EQUIVALENTS:

A - 00,35,68	I - 04,34,81	R - 16,51,82	CH - 26,59,90
B - 01,36,67	J - 09,44,75	S - 17,52,83	Q - 25,60,91
W - 02,37,68	K - 10,45,76	T - 18,53,84	Y - 26,61,92
G - 03,38,69	L - 11,46,77,	U - 19, 54,85	X - 27,62,93
D - 04,39,70	M - 12,47,78	F - 20,55,86	Ä - 28,63,94
E - 05,40,71	N - 13,48,79	H - 21,56,87	Ö - 29,64,95
V - 06,41,72	O - 14,49,80	C - 22,57,88	Ü - 30,65,96
Z - 07,42,73	P - 15,50,81	B - 23,58,89	

EXAMPLE OF HATTED SUBSTITUTION WITH SEVERAL EQUIVALENTS

A - 52,84,25,87	I - 81,56,86,21	R - 34,27	CH - 18
B - 49	J - 42	S - 53,41,08	Q - 07
W - 38,92,67	K - 19,78	T - 58,40	Y - 93,96
G - 60	L - 17	U - 89	X - 06
D - 15	M - 01, 35	F - 37	Ä - 63
E - 47,51,59,24	N - 71,68,29	H - 80	Ö - 23
V - 97	O - 85,43,10,39	C - 64	Ü - 91
Z - 45	P - 54,31, 14	B - 73,90	

c. Expanded Substitution

In this variant the number of clear text symbols is increased by figures, punctuation marks and bigrams (which are mostly short words); this has the effect of still further confusing the statistical picture of the cipher texts. But even in this case there are no serious difficulties for the cryptographer.

As in the above-mentioned examples, it is possible to distinguish between hatted and non-hatted forms of expanded substitution.

Doc ID: 6587327

EXAMPLE OF THE RANGE OF SYMBOLS IN AN EXPANDED SUBSTITUTION

A	N	C	6
B	NA	O	1
T	NE	CH	2
G	NO	Q	3
D	O	Y	4
DO	OB	X	5
EE	P	J	6
V	PO	U	7
ZA	R	E	8
I	S	(.)	9
IZ	T	(,)	ØØ
K	U	(-)	ØØØ
L	F	(?)	
M	HE	No.	

All substitution variants occur as a rule as ad hoc or emergency keys. After the abolition of PT-tables for the wireless operator at the keying device (see below) they occurred especially often; latterly, however, their use has again been sharply curtailed.

It is not really possible to talk of a "reciphering procedure" with these simple keys. It does of course happen that simple non-hatted substitutions, which in themselves are unrelated, appear as reciphering variants and are so listed by a registry.

2. The Table

The table is a cipher in an exactly determined form, the nucleus of which is, in most cases, an alphabet. The predetermined form allows of the application of reciphering rows and thereby of its more or less long-term employment without more than ordinary risk of compromising the basic key.

Sometimes the individual items in the table already have more than one meaning; in such a case the correct interpretation of the cipher group is guaranteed by special switch groups.

It is unnecessary to go into details of the different forms of the resulting picture, since everything written in the next chapter (the code-book) applies in equal measure to the table.

It should be pointed out that there is in practice no clear-cut differentiation of the terms "table" and "code-book". The SOVIETS themselves, for instance, designate some cipher instructions of several pages (i.e. small code-books!). "tablica" and not "kod".

Attempted definition: the table is a single page cipher instruction in reciphering which at the most two independent processes may be used.

3. The Code Table (Signaltafel)

In contrast to the table, the code table is in most cases a cipher medium adapted to a specialized purpose (e.g. air to ground traffic of individual special units, meteorological reports, reconnaissance etc.). The task of enciphering letters recedes into the background or is even impossible, because the basic text in most cases looks an alphabet and consists of only stereotyped orders, reports and queries.

Doc ID: 6587327

The fact that the code table is usually a small one, means that the items are not arranged alphabetically and can often not be so ordered, because the table consists of items made up of several units joined together. Nor is alphabetical arrangement necessary, because the small number of items can be envisaged at a glance .

The province of the code table is air to ground and air to air traffic. It is mostly written out by hand and, as a rule, intended for one operational flight only. Reciphering is superfluous, because in these circumstances it is no more trouble to remodel the table.

The security of the code table is very high. Successful reconstruction can be achieved only by close co-operation between wireless traffic evaluator, content evaluator and cryptographer. The man best suited to this task is not the cryptographer but the traffic evaluator who achieves his object most rapidly on the basis of the daily reports on the signals traffic involved.

Captured copies, which are comparatively often available (from aircraft which have been shot down or which have made emergency landings) are of very little value owing to the short length of time during which such tables remain in force.

Doc ID: 6587327

EXAMPLE OF AN AIR TO GROUND CODE TABLE
(RECONNAISSANCE)

250	wylet
251	kurs ... gradusow
252	perelet frontowoj linii
253	posadka na a)rodrome ....
254	wynuvdennaä posadka
255	zenitnaä oborona w kwadrate
256	istrebiteli protiwnika w kwadrate

310	sewer	477	pogoda
311	sewero-wostok	478	oblaönostx
312	wostok	479	weter
313	ügo-wostok	480	widimostx
314	üg	481	[illegible]
315	ügo-zapad	482	dovdx
316	zapad	483	sneg
317	sewero-zapad		

600	ball	830	dwivenie
601	km	831	skoplenie wojsk protiwnika
602	metr	832	otdelenie
603	kwadrat	833	wzwod
604	öas	834	rota
605	minut	835	polk
		836	diwizia etc.

450	podwoda	857	gorod
451	awtomachina	858	derewnä
452	tank	859	w lesu
453	pehota	860	opuchka lesa
454	konnica	861	na chosse etc.
455	artileriä		
456	art.ogonx		
457	awiaciä		

000 / 030   530 / 560   769 / 799   alphabet with three equivalents.

Figures are given in clear.

Doc ID: 6587327

4. The Basic Book.

The basic book is the principal enciphering medium of the SOVIET Air Force (especially in the case of its most important branch from the intelligence aspect, viz. the ground organisation). The external form and the internal construction of the basic books used are varied in many ways; all variants, from the strictly non-hatted basic book with a few hundred items to the hatted basic book with up to 30,000 items, are present in many different forms.

a. With reference to the relative arrangement of the various basic book significations, the following variants may be distinguished;

aa. The Non-hatted basic book.

All the words in the basic book (viz. items) are in strictly alphabetical order, both in respect of the initial letter as of the following letters. Figures and punctuation marks also are sometimes treated as words and brought into alphabetical sequence.

Once this principle has been recognised, cryptographic work is considerably simplified; restoring relative data to then true values, searching for reciphering and interpreting new basic book significations (decoding) can be made into more or less mechanical processes.

bb. The partly hatted basic book

With this variant the strictly alphabetical character of the basic cipher is disturbed, in which case two possibilities exist;

either; all significations remain in alphabetical order as regards their initial letter, but the position of composite items varies with different initial letters.

Example: Order of items (P) on pages 1 and 2 of the basic book.

1st page: PN 1-43, PB 1-12, PP 1-45

2nd page: PP 46-95, PX 1-3, PR 1-48

(In this example each page has 100 lines. The significations beginning with any one letter are numbered consecutively according to their alphabetical sequence).

This variant first occurred during the war and is fairly frequently used. - Cryptographic difficulties are increased. In particular, the true page values of the code-book can only be restored when items with a single initial letter cover two pages of the code-book (location of adjacent pages). Should this not be the case, then the true page values can be restored only on the basis of a recognised system in reciphering.

or: the sequence of the initial letters in the basic book is preserved, but the significations with a given initial letter are in each case hatted among themselves.

Doc ID: 6587327

Example: Order of items on page 1 of the basic book.

PA 7, 15,2,43,25,1 etc.

PB 10,2,8,3,1,12,7,9,11,5,4,6.

PW 24,30,11,17,1,8 etc.

This form occurs comparatively rarely and then chiefly with small basic books in which the items under one initial letter can conveniently be covered at a glance.

While in the case of this variant, there is no difficulty in restoring the true page values, the lines can be matched with the original only if systematic reciphering rows are used.

cc. The hatted basic book.

In this case the significations are not arranged alphabetically at all, or at the most are arranged according to subject matter, (e.g. items for meteorological reports, addresses and ranks, units, reconnaissance reports etc).

To allow of reasonably fast working, either the basic book must be relatively small or else enciphering is done from an alphabetically arranged conversion copy of the basic book. The SOVIETS limited themselves to fairly small basic books of this kind: the introduction of conversion copies was never detected.

The reconstruction of hatted basic-books is naturally considerably more difficult; the same applies to the task of determining true values. In this case also, help is afforded only by some kind of systematic construction (reciphering rows, systematic arrangement of figure items in the code book). Similarly, decoding is a more laborious process.

b. In respect of enciphering of figures, the following forms of basic book may be distinguished:

aa. The basic book without figure items.

The basic book provides no means for enciphering figures. In such a case, either the figures must be given in clear, or else they are altered according to some auxiliary cypher outside the basic book (figure reciphering tables). Reciphering of figures by letters and by word items in the corresponding basic book was only very rarely observed.

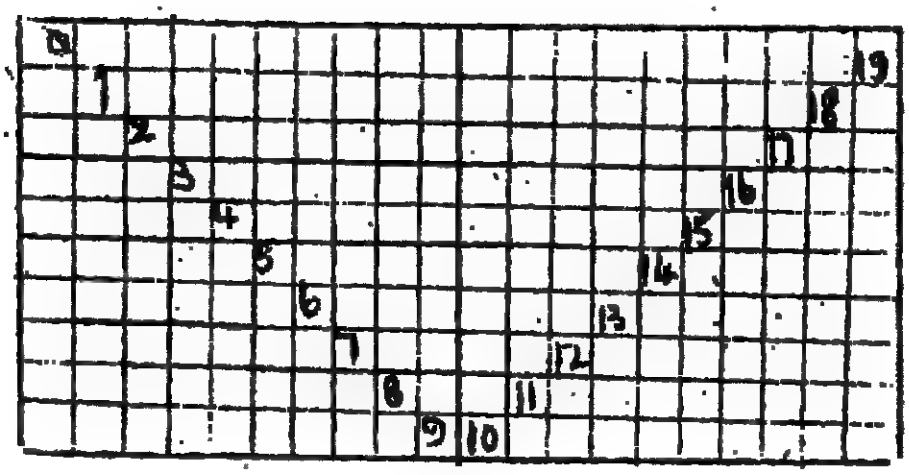
In order to prevent figures in clear, or figures converted according to an auxiliary cipher outside the basic book, being distinguished in the normal enciphered text, these figure groups are assimilated to the cipher text as far as the size of each group is concerned. But in order to avoid misunderstandings in deciphering the signals, basic books are occasionally provided with special code (SIGNAL) groups which indicate figures in the cipher text.

Doc ID: 6587327

bb. The basic book with systematically arranged figure items.

The figure items are for the most part distributed in the basic book according to an easily recognisable system.

Example of systematic distribution of figure items on two adjacent basic book pages:



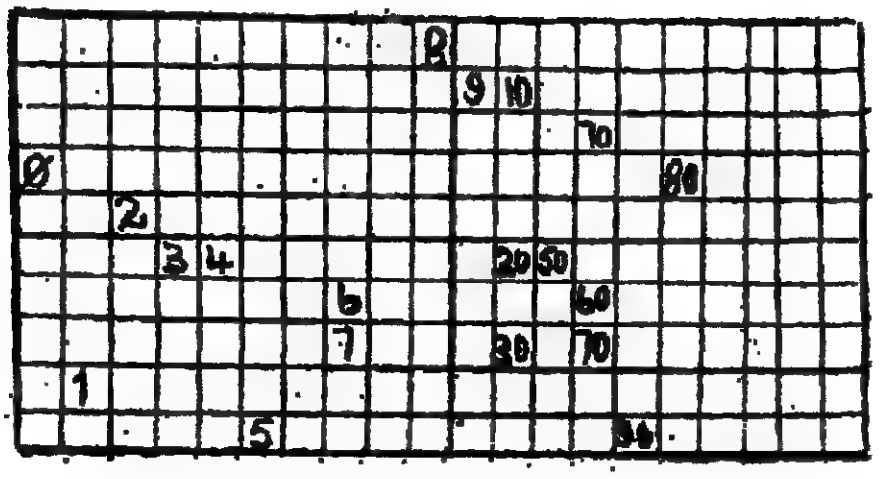
In the case of this variant, the cryptographer is also enabled to restore the basic book to basic values, if it should be hatted. - Such basic books were fairly frequently noticed.

On the other hand, it is also possible to confine the figure items to one special portion in the body of the basic book: the last pages of the book are generally used for this purpose. In this case the unknown figure items can be just as easily identified as if they are systematically arranged in the basic book, but the figures cannot so easily be used for restoring the true page values.

cc. The basic book with a partially systematic arrangement of figure items.

As a rule, the figure items are scattered through the basic book in ascending or descending order, but the intervals between adjacent figures are selected on a purely arbitrary basis.

Example of a partially systematic arrangement of figures:



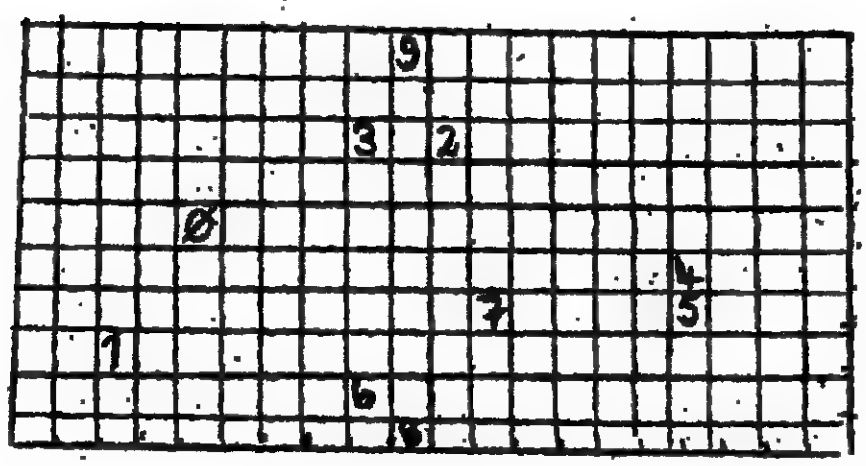
Doc ID: 6587327

Here, unidentified items are often recognised as figures only with great difficulty; in addition, restoration of true values by means of figure elements is possible only to a very limited degree.

dd. The basic book with unsystematically arranged figures.

The position of the individual figure items within the basic book is selected on a purely arbitrary basis, both as regards their figure value as well as the intervals between adjacent figures.

Example of a hatted arrangement of figures:



Both the recognition of figure items and their interpretation entail considerable difficulties. Similarly, it is impossible to reconstruct the true values on the basis of the figures.

Such basic books, however, occurred but rarely; they were always of small size.

c. With regard to their internal structure, the following distinctions may be made:

aa. The basic book without special sections.

These are primarily strictly non-hatted data, which must dispense with all special sections on account of the principles on which they are constructed.

bb. The basic book with special sections.

Most basic books have, generally on the last pages a smaller or greater number of special appendices. The following kinds of special sections have been observed:

Doc ID: 6587327

Figure items,
Names of months,
Times,
Punctuation marks,
Switch groups,
Addresses and signatures,
Units,
Weather items,
Type designations (aircraft, engines, M/T, arms, ammunition, wireless stations etc).

In extreme cases a basic book may consist exclusively of special sections; to all intents and purposes it is then a code (SIGNAL) table.

It is often extremely difficult to interpret the items of such special sections with exactitude.

d. The following group of basic books can be distinguished on the basis of the structure of the different basic book items:

aa. <u>The basic book with items having only one meaning.</u>

Every item in the basic book has one meaning, i.e. in one recipherment, a given cipher value will always have the same meaning.

Such basic books were the rule before the war, but of latter years they are being used less and less.

The frequency of a group in the statistical picture is the true one: if a cipher group occurs often, this means that within the cipher text one and the same signification has in fact been enciphered that number of times.

bb. <u>The basic book with items, all of which have several meanings.</u>

Every line of the basic book has two or three meanings, i.e. every cipher value can have two or three different interpretations according to its position in the message. In such a case, however, the actual meaning of every cipher group must be guaranteed to the decipherer by inclusion of special switch groups.

The following switch groups have occurred in basic books:-

(C) - "Read the whole item",
(S) - "Read only the initial letter of the item",
(Z) - "Read the figure value of the item",
(L) - "Read the left side of the item",
(R) - "Read the right side of the item",
(KS) - "End of letter text",
(KZ) - "End of figure text",

Sometimes the above meanings are varied:

(SZ) - "Read the initial letter or figure",
(KSZ) - "End of letter or figure text".

Doc ID: 6587327

The amplifying groups required in the basic book can have either one or several meanings. If one meaning, they are fairly easy to find and interpret. If they have several meanings (and on occasion they were found to have 30-40 meanings) identification is very difficult - in so far as the amplifying groups are not systematically arranged in the basic book or else according to set rules or arbitrarily.

Example of an item with several meanings.

1st Variant:

		7
3	P	pad
8	P	padota
6	pa	paduo
Ø	paJ	paduci
1	PE	payyr

The rows of the basic book are divided into left and right halves. The left and right halves have different significations, but they are mostly in some sort of relationship: for instance, the initial letter of both significations may be the same. The corresponding amplifying groups must be: "Read the left or right side of the item."

Example of an item with several meanings:

2nd Variant:

aJpaJpom
ba
baza
baT
bao
bE
bEA

The rows of the basic book are apparently occupied by one signification, but by using appropriate amplifying groups it is possible to read the whole item or only its initial letter. With this type it is therefore possible to assign several meanings to one letter.

The number of items of a basic book can be doubled or even trebled by the introduction of items having several meanings. Thus, with three-figure groups for instance, it is possible to express nearly 2000 or 3000 significations in a simple form, or correspondingly fewer concepts in composite form, instead of a maximum of 1000 significations as hitherto. This naturally distorts the statistical picture and makes it less suitable for cryptographic investigation, because on the one hand a given cipher group loses its absolute meaning, while on the other hand a given signification (especially letters) can be expressed by a more or less large number of different cipher groups.

This type of basic book came very much to the fore during the latter years of the war.

e. The two following subdivisions may be made on the basis of the frequency of identical items in a basic book:

aa. The basic book in which only one item is used for a given signification.

Every signification occurs only once in the basic book, i.e.

Doc ID: 6587327

the signification "aircraft" or the letter "E" are entered only once in the book.

In this case the statistical picture is clear and unambiguous, so long as no complicated reciphering subsequently blurs it.

bb. The basic book in which several items are used for a given signification.

In order to confuse the statistical picture, significations in common use are inserted several times in the basic-book. This applies particularly to frequently recurring letters and to short words, punctuation marks, figures and amplifying groups.

For multiple enciphering of letters, however, the above-described basic book with items, all of which have several meanings (enciphering of initial letters) is used with far greater effect.

It is usual to keep a few lines of the basic book free for new items. Added items naturally spoil the alphabetical sequence of items in nonhatted basic books to a greater or lesser degree.

The above-described kinds of basic book can of course occur in combined forms. See the chapter entitled "Examples of SOVIET Air Force cipher systems."

With the great majority of basic books of normal size (500 to 1500 items) it is impossible to discover the individual item from the basic book unless the corresponding reciphering rows have been placed alongside the basic book, i.e. the item is not yet indicated in the basic book itself by a figure value; it is not numbered.

5. Separate code tables.

a. Coding table for addresses.

At times special cover-tables are used in a large unit (mostly an Air Army) to encipher addresses and signatures, and this independently of the actual enciphering of the message.

Recipherment of individual table items does not as a rule occur, or if so, only very rarely.

Interpretation of these address cover groups can be done by means of the contents of messages already broken, but the interpretations are not always very precise.

Example of an address cover-table:

325	The (to the)	AOC Air Army.
327	The (to the)	Chief of Staff of the Air Army.
329	The (to the)	Director of Supplies of the Air Army.
330	The (to the)	Director of Signals of the Air Army.
		etc.
347	The (to the)	AOC Air Corps
349	The (to the)	AOC Air Division
350	The (to the)	OC Air Regiment
		etc.

Doc ID: 6587327

366 The (to the) OC RAB*
368 The (to the) OC of the BAO*
etc.

[Trns: * RUSSIAN abbreviations]

b. The coding table for a/c types.

Similarly, aircraft types were also enciphered according to a special table. This table, however, was valid everywhere at the front.

These aircraft cover groups were used not only in stereotyped strength returns but also occasionally in messages enciphered according to a regional cipher system.

These tables also were reciphered only at rare intervals and then non-hatted or partially hatted rows were often used.

These tables were broken into directly through the complete text of a broken message or else by means of the files of the evaluation department.

6. Proformas

For enciphering stereotyped reports, so-called proforma sheets ("proforma No....") were used: they were valid locally.

In the first place they concerned the following types of report:

Strength (personnel),
Strength (aircraft),
Strength (M/T);
Movement of fuel,
Movement of Ammunition,
State of Airfields,
Medical condition of the men, etc.

The columns of the proforma are numbered in sequence, the report values (mostly figures) are given in clear, only words and sentences are enciphered, often by the regional enciphering method in force.

For differentiating between various proformas within a district, they are given a serial number; sometimes they are also announced by a special code group, either alone or additionally.

Example of an aircraft strength return:

Proforma No. 5 (aircraft strengths)

1)	Unit number	27.AP/29.AP
2)	Total number of aircraft	29 32
3)	serviceable:	25 24
4)	Type I,	23 20
5)	Type II,	2 3
6)	Type III,	0 1
7)	unserviceable:	3 4
8)	Type I,	2 4
9)	Type II,	1 0
10)	Type III,	0 0
11)	under repair away from unit:	1 4
12)	Type I	0 2
13)	Type II,	1 1
14)	Type III	0 1

Cipher message: 1) 27, 2)29, 3) 25, 4)23, 5)2, 6)0, 7)3, 8)2, 9)1, 10)0, 11)1, 12)0, 13)1, 14)0, 1)29, 2)32, 3)24, 4)20, 5)3, 6)1, 7)4, 8)4, 9)0, 10)0, 11)4, 12)2, 13)1, 14)1 +

Doc ID: 6587327

Example of a report on the state of airfields:

1/ Airfield according to map grid or enciphered according to the method in use by the unit,
2/ Size of airfield (total),
3/ Size of runway,
4/ Serviceable or not? (clear text or cipher).

Cipher message: 1/46355k 2/1000x800 3/200x40 4/net,
1/49512u 2/1200x1000 3/150x60 4/da.

The working out of proformas was the task of a small group of workers in the Evaluation Department. The personnel, however, were mostly from the cryptographic department: in addition, cooperation between these men and the cryptographers was of the closest for technical reasons.

7. Lettered coordinates.

There were both general and regional lettered coordinates. Their contents also were handled by the evaluation department. - The author remembers no details.

The recognized specialist for lettered coordinates (and for proforma reports) was Reichsangestellter* (later Feldwebel) Paul KAMMLER, who handled these branches in the course of his duties with II/353 in a manner which was a model for the whole of the east and which has never been surpassed. K. entered the hospital at ORANIENBAUM near DESSAU a few weeks before the surrender, suffering from blood poisoning; the author knows nothing of his fate.

8. Meteorological ciphers.

Before the war the SOVIETS enciphered weather reports according to the COPENHAGEN cipher. During the war, however, it was in addition reciphered with a subtractor table which permuted every six hours by hatting the table columns; furthermore, the starting points in the table were similarly altered

The subtractor tables were changed at irregular but short intervals.

The Listening Service in the east was never concerned with breaking these specific weather messages. This was the task of the Director of Meteorological Services with the Ops. Staff (Ob.Insp. NAUMANN u. ARNDT).

Only in 1944 was a planned deciphering of intercepted meteorological messages instituted at the request of the LUFTFLOTTEN. This was done in the Abteilungen of Regiment 353 by one or two meteorological cipher personnel belonging to the Director of Meteorological Services. The six-hourly permutations were dealt with exclusively in the Director's offices and regularly broadcast to the Abteilungen.

The meteorological group in each Abteilung was likewise subordinate to the evaluation dept.

[Trns.* a grade of civil servant.]

Doc ID: 6587327

B. RECIPHERING METHODS.

The basic cipher is determined by its external form and by the sum total of 15 items. If these items are numbered right through and the clear text is then enciphered with these basic figures, the sum of such figures (the statistical picture) yields a fairly accurate picture of the basic key. External form and contents can be seen as it were thinly disguised by a veil.

All reciphering therefore has as its purpose so to alter the enciphered text that not only are certain figures replaced by others, but so that the statistical picture of the final cipher text shall:

1. disguise as far as possible the true form of the key used, and
2. break up the frequency of the original language as radically as possible.

To achieve this object, the SOVIETS use the following kinds of aids to reciphering:

1. reciphering rows to place alongside the text,
2. substitution tables,
3. adder tables.

1. Reciphering Rows.

In the case of most SOVIET ciphers, the various items are not designated by basic figures. To read off an item in such cases one must place alongside them all necessary reciphering figures or else write them in.

In the case of small keys it is common practice to write in the correspondingly short reciphering rows in the appropriate squares of the key and to erase them after use or when they have lost their validity. This method, however, is practical only when each reciphering method is in use for a long period (say 24 hours) and when it cannot during such a period be replaced at will by other methods.

If, however, the key is a comprehensive one, the number and length of reciphering rows are considerable and changes in reciphering must frequently be made, then a whole series of reciphering rows is generally prepared in advance for a given period. These series of rows are then applied to the original cipher data according to the existing rules. The SOVIETS call the series of rows "wkladychi".

Apart from the number of symbols in the individual members of a row, the following rows may be distinguished:

a. When comparing individual members of a row:

aa. The systematic row.

Examples:

continually ascending: 25 26 27 28 29 30 31 32 33 34 35 36 etc.
continually descending: 81 80 79 78 77 76 75 74 73 72 etc.

Doc ID: 6587327

in ascending arithmetical progression: 15 20 25 30 35 40 45 50 55 etc.

in descending arithmetical progression: 77 66 55 44 33 22 11 00

bb. The partially systematic row.

Examples

ascending in irregular intervals:

04 06 07 11 14 21 26 29 30 39 etc.

descending in irregular intervals:

75 71 69 66 65 64 58 52 47 etc.

unsystematic rows with systematic fragments:

11 12 13 14 15 77 66 55 44 18 16 22 24 26 28 etc.

cc. The unsystematic row.

With such rows, analysis fails to discover any obvious facts.

b. When comparing rows of the same kind, i.e. such as are intended for the same reciphering process, in regard to their mutual relationships, the following possibilities occur:

aa. The rows are cyclically permuted.

All rows are only cyclic permutations of a single row.

Example:

Basic row: 1 0 9 4 3 7 2 6 8

Permutations:

0 9 4 3 7 2 6 8 1
9 4 3 7 2 6 8 1 0
4 3 7 2 6 8 1 0 9 etc.

If one row of the series is available, all other permutations can be reconstructed from it. When reconstructing a new row only one value is necessary to get out the entire row. The basic row can, however, have more elements than the normal reciphering row.

Example

Basic row: 27 44 28 56 03 81 63 00 74 92 93 48 50

Variants = reciphering rows:

03 81 63 00 74 92 93
74 92 93 48 50 27 44
50 27 44 28 56 03 81 etc.

Doc ID: 6587327

bb. The rows hang together systematically (magic squares).

The rows of a series may not have the same value in the same position. If for instance the initial figure of a row is 7, then no other row (i.e. in practice not more than nine) may have an initial figure 7.

Example of a magic square (Latin square (SYSTEMQUADRAT)):

	0	1	2	3	4	5	6	7	8	9
0	9	5	4	0	2	7	3	1	6	8
1	1	9	6	5	0	8	4	2	3	7
2	3	7	2	8	6	0	8	5	4	1
3	6	2	5	1	3	9	0	8	7	4
4	8	1	3	6	9	2	7	4	0	5
5	4	0	8	7	1	6	5	3	2	9
6	7	4	1	8	5	3	2	0	9	6
7	2	6	0	4	8	5	9	7	1	3
8	5	3	7	2	4	1	6	9	8	0
9	0	8	9	3	7	4	1	6	5	2

In this case the rows of a series cannot easily be deduced from one single row, but reconstruction of a few rows is sufficient to facilitate the task of finding the others.

cc. The rows are independent of one another.

The only common factor is the number of members, otherwise they are completely unrelated.

In this case every row must be discovered separately.

c. Comparing the individual members of a row on the basis of their validity leads to the following conclusions: there are rows with members having several values and members having only one value.

aa. The row with members having only one value.

All the rows given so far can serve to illustrate this form.

bb. The row with members having several values.

In such rows the various items have no absolute value, but several equivalent values. The individual values of a member of a row can be used indifferently when reciphering.

Example:

The 5 columns of a table are to be reciphered by single-digit numbers. Since, however, 10 single-digit numbers are available, every individual member can be given two values. The row could then be rendered as follows:

5/7 1/9 6/8 0/4 2/3

If the table has only 4 columns, however, it is even possible to give some members three values:

2/4/6 0/3 1/7/8 5/9

Doc ID: 6587327

But if several adjacent figure values are chosen to represent individual members of the row, then one speaks of "figure range" reciphering (Bereichsüberschlüsselung).

Example of a row in "figure range" reciphering.

86-97 41-52 07-15 63-69 53-62 23-26 16-22 70-85 98-06 27-40

In this row the values 63, 64, 65, 66, 67, 68 and 69 would for example be the reciphering figures for a single value of the key.

By the use of reciphering rows with members having several values, the key itself appears larger in the statistical picture of the cipher text than it actually is - the statistical picture is thus more or less strongly blurred.

d. Also when comparing different kinds of reciphering rows of a reciphering system, i.e. rows used for different reciphering processes (e.g. one row is used for rediphering the pages and another for reciphering lines), the same observations as in paragraph C may be made:

aa. The rows can be built up out of one another, they are cyclic variants;
bb. The rows hang together in some way;

Example: while the A-rows of a two-figure key are read vertically from a latin square, the B-rows in the same square are read horizontally.

cc. The rows are completely unrelated.

The effect of these alternatives on cryptography is the same as in paragraph C.

2. Substitution Tables.

While the row is placed alongside the key page and the latter contains no (basic) figure values for its items, the necessary precondition for reciphering by substitution table is the presence of such basic figure values in the key page.

The items are first of all read off from the key page together with their basic figure values and then these basic values are changed according to a substitution table, i.e. reciphered.

Example of a substitution table.

	0	1	2	3	4	5	6	7	8	9
0	29	12	68	46	55	40	07	79	38	90
1	13	03	54	89	18	39	61	34	27	50
2	19	63	09	35	66	28	52	84	11	76
3	36	91	37	60	00	02	67	48	23	17
4	72	16	87	26	51	85	33	22	05	59
5	47	88	45	53	81	06	58	65	49	83
6	64	01	44	15	71	32	94	75	41	74
7	10	62	96	20	04	99	56	25	98	42
8	30	93	86	57	08	70	95	73	31	77
9	82	21	80	43	78	97	92	14	27	69

When reciphering single-digit values outside the key, one speaks of a substitution row.

Doc ID: 6587327

Example of a substitution row:

Figure group of the key: 0 1 2 3 4 5 6 7 8 9
Cipher text: 7 6 5 8 1 9 4 0 2 3

Substitution tables (or rows) are used only very rarely in SOVIET methods and therefore need no further elaboration in this context. See description of the "okk-5" on page 37.

3. Adder Tables.

The use of adder reciphering was never observed in purely air traffic systems. Only the general five-figure systems of the RED ARMY, which are also used by the Staffs of the Air Force, use this form of reciphering.

In reciphering with adders, the cipher text which has been enciphered by using the basic figures of the key is reciphered by using the so-called adder: in this case the adder takes the form of a row of figures, in which the latter are grouped purely arbitrarily and in which the various adder figure groups do not recur.

Example of reciphering by adder:

Basic figure cipher text:	81024 10231 67024 18729 56039 82465 67024 56039 81024
+ adder:	70568 39084 54022 77757 13900 57337 82582 02223 97574
final cipher text:	51582 49215 11046 85476 69939 39792 49506 58252 78598

(obtained by non-carrying addition of figures in the same column).

The frequencies in the basic figure text have been completely broken up by the adder; if frequencies occur in the final cipher text, then in 99 cases out of 100 they are "bogus", i.e. identical cipher groups have different meanings.

If the adder groups are added to the basic figure text when enciphering, then these groups must be subtracted (non-carrying) from the cipher text when deciphering. Conversely, if the subtractor groups were subtracted when enciphering, they must be added when deciphering.

a. The adder table which is used several times ("obqij bloknot")

It consists of a few hundred arbitrarily assembled five-figure groups (10x30); every individual adder group can be denoted by different combinations of a two or three-figure number (the indicator) and thereby designated as being the initial group in the reciphering process.

Every adder table similarly receives its own recognition number.

Such "universal adder tables" were intended for reciphering several messages; they usually remained in use for some weeks, during which time only the starting group was varied for each message.

Doc ID: 6587327

If a number of messages were enciphered with the same adder table - even when different starting points were used - it was possible to reconstruct the table, thus providing the necessary precondition for reading the messages. The work was laborious but fairly mechanical and necessitated very reliable, but not necessarily qualified personnel. While at first (1939) a depth of 10 messages was considered necessary to cryptographic success, one had latterly to be content with 2 messages - and successes were still achieved.

b. The adder table which is used once only ("individualxnyj bloknot").

Individual tables are just as large as "universal" ones but there are no indicators to determine the starting point.

50(?) tables are made up into a "bloknot". The "bloknot" is given a five-figure identification group and the tables are numbered right through.

Every "bloknot" is issued in two copies which are handed to the two stations which are to encipher according to this "bloknot". After the receiving station has receipted a message, both stations destroy the page used for enciphering and deciphering (both copies of which bear the same serial number), and confirm its destruction on the cover of the "bloknot". The purpose of this is in all circumstances to prevent an adder being used twice. This rule was broken only in rare cases, e.g. in the last days of the siege of SEBASTOPOL, because the supply of "bloknots" broke down. On the whole, however, the supplying of all higher HQ's of the RED ARMY with these "bloknots" has been a masterpiece of organisation. In spite of the absolute security of the "individual" tables it must not be expected that the SOVIETS rely exclusively on individual adder reciphering, because the ciphering procedure is very laborious and demands staff having some degree of intelligence as well as practice.

Example of a universal adder table.

	10	17	25	31	39	46	53	69	80	99
173	28476	90416	38410	33552	38496	22987	30416	77465	11100	64599
935	98765	21415	33144	28490	46573	15146	33775	20495	31157	35746
855	35420	77685	14466	87881	usw.*	.....	.....	.....	.....	.....
290	.....	.....	.....	.....	.....					
511	.....									
usw?	....									
	.....									

Trns: * The abbreviation "usw" = etcetera.

Doc ID: 6587327

C. THE CIPHER SYSTEM

The sum total of all the necessary data, auxiliary means and working instructions for completely enciphering (including reciphering) a clear text constitutes the cipher system.

1. The reciphering system.

The reciphering system is the name given to the whole of the rows and tables necessary for completely reciphering a given text, including the instructions for the various reciphering processes, the way of reading cipher groups, for building up the indicator and determining its position in the cipher message, for changing reciphering data and for the use of dummies.

a. The process of reciphering.

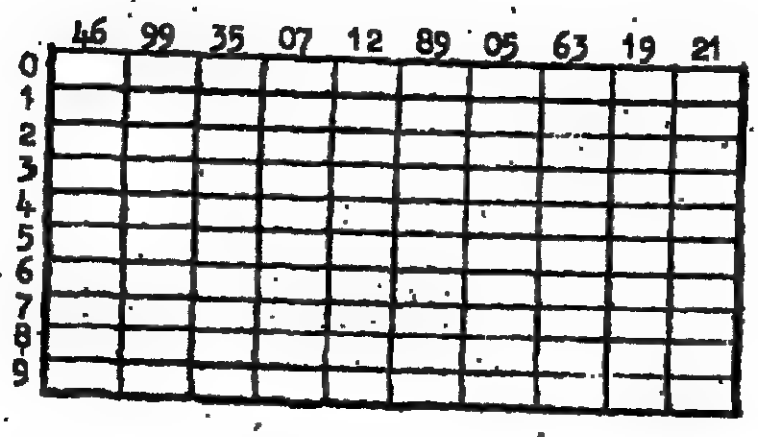
A distinction is made between simple and multiple reciphering according to the number of processes involved.

aa. Simple reciphering.

In this kind of reciphering, the key is altered by one process only, and thus by means of a single reciphering row.

EXAMPLES:

1. A 10 x 10 table is reciphered by altering the columns of the table: this is done by placing alongside a row consisting of 10 two-digit members. The lines retain the values inscribed in the table.



2. A 40-page code book is altered by reciphering the pages by means of an unsystematic substitution table (i.e. the AB -values of the cipher groups); the CD -values (lines) remain as unaltered basic values of the code book.

bb. Multiple reciphering

In this case every item is altered by several processes: either exactly as many rows are available as there are processes or else the number of rows is less, in which case an item, although occurring in several different positions, will be reciphered by the same row.

Doc ID: 6587327

EXAMPLES:

1. In a four-figure method (the cipher groups are then usually called "ABCD") the A-values (i.e. the pages) are altered by means of one reciphering row, the B-values (i.e. the quadrants) by means of a second row and the CD-values (i.e. the lines) by means of a third row.

2. In another four-figure method both pages and quadrants are reciphered by means of the same row, while the lines are reciphered by means of another row.

While in the first example, the number of processes equals the number of rows used (3 : 3), the second example again involves three processes but the use of only two rows.

The higher the number of processes and the greater the number of reciphering rows used, so much greater will be the divergence between the statistical picture of the cipher texts and that of the (fictitious) basic figures of the significations in the code book, i.e. the more difficult the cryptographic process will become.

b. The series of reciphering rows.

All the rows used in one reciphering process are grouped together in series, and each row is given a recognition number. When dealing with a basic row or an adder table, however, every possible starting point must also be determined by a recognition number.

Examples:

1. Series of 10 rows, each with 10 single-digit elements:

Recognition number										
0	0	4	5	9	6	7	3	8	2	1
1	1	5	0	3	2	4	7	9	8	6
2	0	4	5	1	6	3	8	9	2	7
3	9	5	8	1	0	2	4	7	6	3
4	0	1	2	6	9	5	8	4	3	7
5	7	3	0	9	5	1	2	4	8	6
6	7	1	0	5	4	2	8	9	6	3
7	1	8	9	3	2	6	7	0	4	5
8	3	7	0	8	4	6	2	9	5	1
9	8	4	6	3	2	5	7	9	1	0

2. Basic row.

	8	1	7	3	6	5	4	2	0	9
Starting recognition number.	0	1	2	3	4	5	6	7	8	9

Doc ID: 6587327

The choice of starting point can be expressed either by the figure value of the first element of the row or else by special starting recognition numbers which naturally do not agree with the figure value of the corresponding element of the row, nor do they need to agree. In the first case, the starting recognition number for the row

7 3 6 5 4 2 0 9 8 1

would be "7", in the second case it would be "2".

2. Change of Reciphering Tables

The purpose of a change of reciphering medium is to break up the mass of material enciphered according to a given method in order as far as possible to render more difficult or even altogether impossible a statistical comparison of the various messages. Therefore the more frequently the reciphering medium is changed, the more difficult will the breaking process be.

a. Infrequent change of reciphering tables

In the case of infrequent change, viz. about every 24 hours or even less often, the reciphering tables are generally laid down in advance by the superior authority for a period of a week or a month at a time. This means that the individual cipher message need not contain any special indication of the reciphering medium chosen.

b. Frequent (individual) change of reciphering tables.

If on the other hand the reciphering table is to be changed often, say for every message, the encipherer is enabled quite independently and arbitrarily to chose a reciphering table from the system at his disposal. This entails the necessity of advising the station at the other end of the reciphering table used by including a special key group, i.e. the indicator, in the body of the message.

This type of reciphering has triumphed in the latter years of the war, whereas before the war long-term reciphering tables, i.e. such as were laid down beforehand and not indicated in the message, were in general use.

c. Change of figure values in the reciphering system.

If the reciphering system is in use for a fairly long period the figure values of the different series of rows are altered at given intervals, mostly once a month; this does not involve any change in the general working instructions for the reciphering process.

After a certain time has elapsed the available rows do not coincide with the message indicators and they must then be built-up afresh.

d. Change of reciphering system

It was repeatedly observed, especially in the case of the

Doc ID: 6587327

southern Air Armies, that after a system had been in use for a fairly long time, the key data did indeed remain in force but the reciphering system had been so radically altered that it was several weeks before both sets of key data were seen to be identical. Even externally the change was very marked; thus for instance, messages enciphered by means of a 1000-item key appeared in four-figure groups, then the reciphering system was so altered that the method assumed a three-figure aspect and finally, due to a fresh change of reciphering system and to the introduction of two-figure dummies, a five-figure method was developed.

This fact demonstrates how very inadequate is the classification of SOVIET methods according to the appearance of the cipher groups.

3. The key group (the indicator).

The recognition numbers of all the rows, tables and sometimes starting points used for one recipherment are combined in a so-called key group or indicator according to a prescribed system.

a. The indicator in the cipher message.

The position of the indicator in the cipher message is prescribed and is generally invariable for a given system. Only with the five-figure adder messages sent before the war (general "bloknot") was the position of the adder starting group in the message changed daily (1st-10th position).

The indicator is normally placed at the beginning (preamble of the message or in one of the first positions in the body of the cipher text) or at the end of the message.

Sometimes it is repeated as a safeguard; then it may be placed both at the beginning and at the end of the message.

In order to disguise the indicator, at least to some extent, the number of its figures is made equal to that of the cipher groups. Furthermore, the equivalence of two indicators can be very strongly disguised by using dummies for, or by allotting certain values to some or all indicator figures.

b. Method of reading the indicator

The indicator is usually read in the same way as the other cipher groups. Thus if a cipher group is read ADBC, the indicator is read in the same manner.

The methods of reading may, however, be different. Then the relationship between cipher group and indicator is considerably blurred. In some particularly complex cases it is possible unequivocally to interpret the indicator only a long time after recovering the relative or even the original key data and after recovering a fairly large number of reciepherments.

Doc ID: 6587327

c. Composition of the indicator

In most cases only one indicator is needed; exceptionally two key groups are used to determine the reciphering process.

Examples for the build-up of indicators:

1. ABCD (4-figure method)

AB = serial number of the page-reciphering row (two-digit)
C = " " " " quadrant row (single-digit)
D = " " " " line row (single-digit).

2. ABCD

A = serial number of the page row (two-digit)
B = dummy
C = serial number of the line row (single-digit)
D = " " " " quadrant row (single-digit)

3. ABCD

A = serial number of the page row (two-digit)
B = " " " " line row (two-digit)
CD = dummies

4. ABC

AC = serial numbers (within the given range) for page and line (the same row) (single-digit + single-digit).
B = serial number of the quadrant row (single-digit).

5. ABCD

AD = sector number for coupled page and line row (single-digit + single-digit)
BC = sector number for the quadrant row (two-digit).

6. ABCD

A = serial number of the quadrant row (single-digit)
B = line row = starting point for the quadrant row (single-digit)
C = page row (two-digit)
D = dummy

7. ABCD ABCD

AB(1) sector number for the page (two-digit)
CD(1) " " " " line (single-digit)
AB(2) " " " " quadrant (single-digit)
CD(2) dummy

Doc ID: 6587327

4. The Dummy

To confuse the enemy and to render breaking more difficult, cipher groups and even indicators are padded with figures which have no significance and which need not be taken into account when decipnering.

Sometimes indeed one element in the cipher groups can be deleted when it is not a pure dummy but has been put in solely for checking purposes. These are cases of so-called checking figures.

Example of checking figures:

The 10 columns of a table are reciphered with the following row of figures:

00 16 25 38 47 51 63 74 89 92

The A-values of the two-digit reciphering figures each occur only once in this row, similarly the B-values. Hence the B-values are merely checking figures for the A-values coupled to them (or vice-versa). The B-values therefore serve only to identify or to nullify errors in reception: they can be cancelled without further ado.

5. Method of reading the cipher group (the indicator)

In simple systems the cipher group is read quite simply from left to right. The value of the first element in the group gives the reciphering figure for the largest subdivision of the reciphering data (the page), the last figure gives the value for the smallest subdivision, i.e. the line:

The more complicated the type of reciphering, the more irregular and "crazy" is the method of reading the group.

The method of reading the cipher group is indicated by the first few capital letters of the Latin alphabet, where A always stands for the first element in the group, B for the second, C for the third, D for the fourth and E for the fifth.

Examples of formulae for the method of reading:

A/B/CD = A(page), B(quadrant), CD (line)
AD/B/C = AD(page), B(quadrant), C(line)
A/B/C/DE = A(page), B(quadrant), C(line), DE(dummies).

III. THE CIPHER SYSTEMS OF THE SOVIET AIR FORCE 1937-1945 AND THE SUCCESSES OF GAF CRYPTOGRAPHY IN GENERAL

Preliminary note: Until about 1940 it was hardly possible to talk of special cipher methods of the SOVIET Air Force, because the air units were purely army flyers and subordinate in every respect to the army. For this reason the Air Force was in the same position as the army units, even in respect of its supplies of cipher material.

Doc ID: 6587327

A. 1937-1939

The volume of traffic was on the whole not large and increased only during the periods of the spring manoeuvres and of the autumn exercises. But in any case the amount of traffic intercepted was unsatisfactory owing to the somewhat unfavourable locations of the German Listening Stations. Even so it was possible to work out a very valuable picture of the enemy situation on the basis of the material broken. Traffic analysis hardly played a part during the first few years: it was of little value in view of the intelligencing of the tactical material broken and cannot be compared with the successes achieved by traffic analysis in the West.

1. Practice Messages

It was possible to classify as purely practice traffic a considerable proportion of the messages intercepted.

a. Nonsense practice messages

Many practice messages were recognized as nonsense messages on the basis of their stereotyped composition (standard number of groups, systematic composition of individual groups). They were also frequently designated by a code group in the preamble or at the beginning or end of the message ("u8", 01234, 56789 etc). The apearance of the various groups of a message varied; two to six-figure groups, four and five-letter groups.

Sometimes it was possible to detect relationships between the figure messages. Practice tables were successfully reconstructed; from these, individual practice messages could be read off. The method of reading was determined by an indicator.

b. Tactical practice messages

Tactical practice messages were in evidence among the traffic of all deciphered systems. These messages, too, were identified by the group "u8" in the preamble or by the inclusion in the enciphered text of a suitable indication.

In the case of material used on manoeuvres, there were messages containing stereotyped facts and names, and these kept on recurring. Thus exactly identical messages appeared on two or three different manoeuvres. It must be assumed that there existed a manual containing standard tactical texts and that this remained in use for a fairly long time.

2. The two-figure table in general use.

A two-figure table in general use was, as laid down in orders, intended in fact only as an auxiliary for enciphering contact traffic between the wireless operators at the machine; this was denoted by the name originally given to it by the SOVIETS, viz. "peregovornaÏ tablica devurnogo radista", or PT for short.

Doc. ID: 6587327

But a large number of messages was enciphered by this table, which was the only cipher device available to a large number of persons - even to OR's, and thus to the wireless operators themselves. It is not known whether this was merely due to slackness on the part of the responsible cipher officers, but this is not assumed to be the case. Rather does it appear to have been done on purpose to preserve the staff method (four-figure, see below) in order by all means to avoid a premature compromise of the latter.

The PT table consisted of 10 x 10 squares; most squares had two meanings; two switch groups were used to indicate which meaning attached to the cipher groups. One of the switch groups controlled letters, figures and punctuation marks, the other controlled word and sentence items; the vocabulary was roughly the same as that of the international Q-code groups.

The tables were in use for about a year to 18 months. For examples, see next page.

The tables were reciphered daily with two ten-element single-digit rows. Both the horizontal and the vertical rows were taken from the same Latin (magic) square. As a rule, each Latin square was in force for a month and had validity within a given military district. Very seldom, the rows from the system table were permuted cyclically (or else the rows of many Latin squares were simply cyclic variants).

PT material could as a rule be broken in its entirety. The security of the key was very low; it was mostly a case of simple letter reciphering; thus to all intents and purposes the PT messages were simple substitutions. The systematic relationships between the reciphering rows of a military district could, provided part of these rows was available, lead to a more or less complete reconstruction of the whole Latin square.

3. The three-figure Air Force Code in general use.

A comparatively simply constructed (lexicographic) and simply reciphered code-book was intended primarily for air to ground traffic. This traffic was, however, almost never heard on account of the short range of the airborne transmitters. In addition, this method was also used by ground networks of the Air Force.

As far as I can remember, two methods of this kind were used one after the other.

a. The 1937-38 three-figure Air Force code-book.

The basis of this was a code book of 7 pages, each of which had 100 lines and alphabetical construction.

The pages were reciphered by means of a simple, unsystematic row; the lines (BC) remained constant.

Cipher security was correspondingly low.

b. The 1939 three-figure Air Force code-book ("WAK-39")

10 page code-book, each page with 100 lines also of alphabetical construction, with a few small special sections

Doc ID: 6587327

on the last page. The line numbering in the code-book occurred three times; every row had a different colour (black, red, green?). All three rows of lines were cyclic variants of the systematically increasing figure row 00-99.

The pages of the code-book (not provided with basic numbers in the original) were reciphered once: for reciphering lines only the appropriate colour was indicated, e.g.
3 7 0 5 8 6 4 2 1 9, green.

cipher security very low.

c. The 1940 (?) Air Force code-book.

In a third three-figure code-book of similar construction, the pages and the quadrants (B) were reciphered in two stages: the lines (C) remained constant.

4. The four-figure staff method in general use, so-called "Commanders' Code."

In this method, more comprehensive code-books with about 5000 items were used. They were also constructed alphabetically throughout. Reciphering was done by placing alongside of rows or by means of substitution tables. These methods remained on an average in force for one year.

As a rule, the new method was adopted for the spring manoeuvres and used extensively only while they lasted. This short period sufficed, however, for the method to be developed sufficiently to allow of breaking the traffic intercepted even at a later date - though at times with considerable difficulty. Outside the period of manoeuvres, only an infinitisimally small number of messages was sent, no doubt with the object of preserving the method from being prematurely compromised, as already mentioned above.

a. The 1937 four-figure method (called "Privo")

Code-book with 50 pages, each of 100 lines. Alphabetical construction with a few special sections on the last pages of the book. Figure items similarly at the end of the code-book, in ascending order.

This method was called "Privo", because the highest number of messages was recorded on the staff networks of the VOLGA military district: the messages were as often as not designated by the code-group "privo".

Page (AB) and line (CD) were reciphered by means of the same values. The basic numbers for the pages were 75-99, followed by 00-24; the basic numbers for the lines were 00-99. Two rows of figures were used every time for reciphering: one row had the values 00-49 and the other 50-99. Furthermore, every row was divided in half.

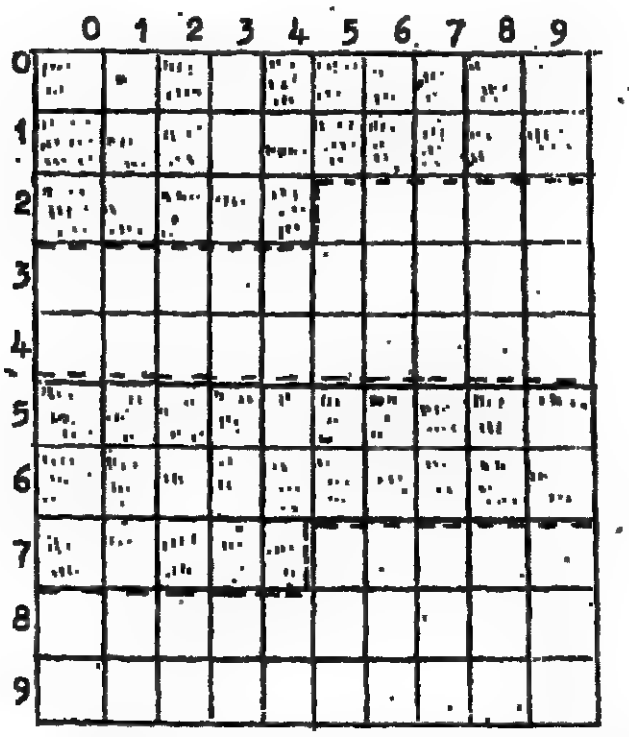
Doc ID: 6587327

Example.

Pages & Lines																									
00-24	23	21	19	17	16	15	13	11	00	02	04	18	20	22	05	03	01	06	10	12	14	07	08	09	24
25-49	25	26	27	46	47	36	35	34	29	31	43	44	45	32	30	28	37	39	41	49	33	38	40	42	48
50-74	61	63	65	73	74	55	57	59	72	50	51	62	64	66	70	71	54	53	52	67	68	69	60	58	56
Pages & Lines 75-99	83	94	84	95	85	96	97	98	99	75	86	76	87	77	88	78	89	79	90	80	91	81	92	82	93

The appearance of the normal four-figure statistical picture was correspondingly pronounced in character.

Example.



The rows chosen for reciphering were determined in the message by an indicator, but I am no longer familiar with the details.

With the small volume of traffic, the security of this key was fairly high: deciphering the messages gave much trouble. Fortunately very many separate letters were enciphered in the texts: these stood out very clearly in the statistical picture.

b. The 1938-39 four-figure method ("okk-5")

This code-book also had 50 pages of 100 lines each, its construction was alphabetical too; there were a few special appendices.

The basic figures in the code-book were reciphered by means of substitution tables in two stages: AB and CD with the same substitution table.

Every substitution table had a recognition number (a four-figure one, invariably with a nought in the first position, e.g. 0451). In most cases, up to 10 tables at a time were issued to the different military districts; their recognition numbers always formed a series, e.g. 0450-0459 or 0780-0789. The table which had been used was indicated at the beginning of the message by giving the recognition number as indicator.

Doc ID: 6587327

The substitution tables were completely unsystematic and in no way interrelated.

Compared with the "Privo" key, the security of "okk 5" was indeed higher, yet if a few good cipher messages were available, the substitution tables could be reconstructed in about 24 hours. Its reduction to basic terms presented no difficulties on account of its systematic construction.

5. The five-figure adder method in general use.

The foundation of this annual method in general use by higher staffs was very comprehensive: the code-book contained 20-30000 significations.

Reciphering was done by applying an adder process to the basic figures in the code book.

Until 1939 the available five-figure material was so small that work on it could not go beyond a general analysis; it was hardly possible to make up adder series.

6. Proformas.

Successful work on proformas before the war was considered impossible and unnecessary from an evaluation point of view: for this reason it was not carried out.

7. Primitive ciphers.

Primitive ciphers which often cropped up were on the whole probably illegal ciphers, i.e. unauthorized ones in use by wireless operators and by certain HQ's. This material was evaluated but yielded no important results.

B. The Occupation of Eastern POLAND by the Red Army in September 1939

At the time of the occupation of Eastern POLAND and of the (admittedly small-scale) battle operations against isolated POLISH units, the volume of messages increased very considerably.

"Okk-5" material formed the bulk of this traffic: it was broken almost 100%. As before, five-figure material was too scanty for successful exploitation.

The outcome of successful cryptography was a comprehensive study by CHI-STELLE on the incursion of the Red Army: this contained a mass of important details and conclusions, particularly concerning the Air Force, and was greatly appreciated by the GAF Operational Staff.

C. The Winter Campaign in FINLAND 1939-40

In a way, SOVIET wireless traffic may be said to have been monitored "on a war basis" for the first time during the winter campaign. The out-stations proved to be too weak to cope with the number of messages intercepted. For this reason the most capable cryptographers at out-stations were concentrated in Section H 1 and all unbroken material was sent currently by teleprinter from the out-stations to CHI-STELLE.

Doc ID: 6587327

1. Two and three-figure messages.

The out-stations themselves were in most cases able to deal satisfactorily with this material by themselves. Nearly 100% breaking.

2. "Okk-5" messages.

Work on "okk-5" material afforded no great difficulty either, although the number of substitution tables in use simultaneously increased considerably. But this material was in the main deciphered by the Section in bulk. The large volume of material made it possible to reconstruct up to 95% of the code-book.

3. The five-figure method.

Since five-figure material was available for the first time in larger quantities, work on it could be undertaken with some prospect of success. A considerable number of these five-figure messages could be broken, but often only after considerable delay: this was entirely due to lack of personnel (only one cryptographer with 10-15 key breakers without linguistic qualifications were on duty at any one time).

Key basis: about 850 pages (ABC), each with 25 lines (DE). The code-book was arranged alphabetically. The pages were numbered consecutively (from 100 to 950), the line designations depended on the C-value: if C was an uneven number, then all the lines on that page were uneven; if C was an even number, then all the DE values were even numbers.

Example: page 467, Lines: 11,13,15,17,19,31,33,35 etc.
page 468, lines: 00,02,04,06,08,20,22 etc.

This system was probably intended to enable errors in reception and calculation to be detected. It represented a welcome aid to cryptography.

Figures were not expressed by items in the code-book but in clear, prefixed by the requisite number of noughts, e.g. 57 = 00057, 164836 = 00001 64836. When calculating adders, figures could easily be identified since they were the only cipher group which failed to conform to the above-described system of CDE-values. In addition, the basic structure of the code-book could be comparatively easily reconstructed on the basis of the figure groups, since date groups and unit numbers were usually interpritable without ambiguity.

As a rule, universal adder tables were used for reciphering; individual ones only very occasionally.

The unit number of the transmitting station was stated in clear at the end of the message.

Address and signature were inserted in the text of the message in any desired position before reciphering, e.g.:

Example:

To-morrow morning between 1000 and 1200 hours (To the O.C. 126 Air Regiment - AOC 4 Bomber Division) the targets in grid-squares 46322, 46414 and 46415 are to be thoroughly bombed.

Doc ID: 6587327

D. Reorganisation of SOVIET Cipher Methods on the Basis of Experiences in the Winter Campaign in FINLAND.

Due to a splendid organisation and to the well-merited attention which it received from the FINNISH HQ's, the highly successful work of the FINNISH Listening Service was often successfully translated into notable operational achievements.

This fact was of course sooner or later bound to become apparent to the SOVIETS also. A printed copy of working directions for SOVIET cipher officers which was captured during the campaign in the East was comprehensive: it studied the lessons of the Winter Campaign and very pointedly criticised SOVIET cipher behaviour. Many a FINNISH military success is attributed to the careless and incorrect use of ciphers. Yet in these arguments, stress is laid first and foremost on the loss of cipher data in the battle line, on the transmission of messages in clear and on the activities of the FINNISH ABWEHR. Only the barest reference is made to the possibility of ciphers being broken.

Be that as it may, the SOVIET Command decides on a revolutionary reorganisation of ciphering systems. The result of this already begins to make itself felt before the start of the Eastern Campaign: it creates great difficulties for the German Listening Service and above all for cryptography, but thanks to the fact that developments had been "kept pace with" for a number of years already, it entails no important or permanent set-backs.

The reorganisation of the SOVIET cipher set-up may be outlined as follows:

1. Abolition of most general methods - institution of regional methods.

Enciphering according to general and comparatively comprehensive methods issued by Department 6 of the RED ARMY GHQ are abandoned, with the exception of the five-figure adder method.

These few methods are replaced by one (or even several) original methods for every wireless network: such methods are as a rule worked out by the cipher officer of the main wireless station. The subordinate cipher offices merely give guidance by issuing directives in general terms and by holding courses for the initial and subsequent training of cipher officers.

Results:

a. The supply problem is excellently solved by these new regulations: the delays in the delivery of cipher data, which had been occasioned by the long lines of communication, are avoided.

b. The cipher instructions can be very well adapted to the special requirements of the separate networks. This also enables the Air Force to introduce their own instructions with a specialised vocabulary.

c. The cryptographer's task is rendered considerably more difficult by this new state of affairs. Even though the separate regional methods become easier by comparison with the general method, the volume of traffic for each method is decreased to such an extent that the method which in itself is less difficult becomes harder to break than difficult methods with a large volume. Since the number of

Doc ID: 6587327

cipher systems to be worked on simultaneously is increased from about 5 to an average of 100, the number of qualified cryptographers with good linguistic qualifications must also be increased out of all proportion at the expense of the auxiliary staff.

d. The identification of messages, which in themselves are enciphered according to a known method, is very difficult owing to the extremely complicated and frequently changing system of call-signs.

2. Shortening of the period of validity of cipher systems.

While the general systems in use before the war were on an average in force for one year, the regional systems are usually superseded after about 3 to 4 months. Yet differences were in part very considerable: while some southern Air Armies in particular retained their systems for periods of up to a year also, other systems were replaced after only a few weeks.

Results: The period of validity was in many cases so short that it became quite impossible to work out the system while it was still in force.

3. Complication of cipher instructions.

Cipher instructions before the war were in the main systematic. War-time methods, on the other hand, become even less so and less transparent in their construction. Items with one meaning are replaced by items with several meanings, enciphering possibilities for letters allow of multiple letter enciphering.

Results: Identifications of new code-book items, decoding and reduction to basic values of the cipher instructions all present far greater difficulties than before the war.

4. Complication of the reciphering systems.

Uncomplicated reciphering processes and rows which are mostly systematic are increasingly replaced by complicated reciphering systems. Row elements with several meanings (sector reciphering) are used more and more frequently.

Results: The perfection of reciphering systems blurs the statistical pictures: reconstruction of cipher instructions and reciphering systems becomes more difficult.

5. Ousting of non-hatted systems.

The undoubted tendency to adhere to systematic construction in the production of cipher instructions and reciphering aids is apparently consciously resisted and kept in check.

Results: The number of "weak spots" is reduced.

Doc ID: 6587327

6. Shortening of the period of validity of recipher keys, introduction of "individual" recipher keys.

Recipher keys which often changed daily and were determined for a long time in advance are replaced by reciphering media valid for one message only and which can be determined arbitrarily by the encipherer.

Results: If the cipher staff work conscientiously, the material for any one system is very much split up, thereby delaying a break-in as well as reconstruction.

7. Introduction of dummies.

The use of dummies was constantly on the increase.

Results: The statistical picture is subsequently falsified by being sprinkled with dummies.

8. Abolition of the two-figure tables in general use for wirless operators.

At first the PT-tables become less systematic in construction. Finally they are abolished and the wireless operators are retrained to use international cipher groups with unimportant modifications.

Results: The disappearance of these tables strongly curtails SOVIET "Private conversations". Apart from the fact that a thorough evaluation of this material could lead to success, the disappearance of material which was excellently suited for training future cryptographers is very much to be regretted from a crypto-technical point of view.

9. Complication of the retained five-figure adder method in general use.

The five-figure code-books were not enlarged but they were made less systematic. The period of validity of each code-book was much reduced. Reciphering with universal adder tables was completely stopped.

Results: Reciphering with individual adder tables, i.e. the fact that a given adder table is used once only, means 100% key security.
While in 1941-42, five-figure material could still satisfactorily be read, successes after this time became less and less frequent proportionately to the disappearance of tables used more than once. In the end, work on five-figure material had to be abandoned by the cryptographers. Even so the interception of five-figure material was not stopped because keeping track of the indicators ("bloknots") had become a valuable basis for interpreting networks and call-signs.

10. The use of machine ciphers.

The use of machine ciphers was undoubtedly tried in individual cases, but on the whole it failed to be adopted. Thus at one time five-letter messages were sent from besieged ODESSA. Analysis revealed that a machine key might be in use, but the volume of traffic was too small for work on it to be successful.

Doc ID: 6587327

During the last few months the wireless traffic of the Corps staffs of the ADD was also carried on according to a five-letter method. Superficial analysis led one to suspect a machine method in this case also. But here too, the volume and the quality of interception were unsatisfactory.

In 1941 or 1942 a captured cipher machine was examined by the Main SIGINT Station. Obviously the examination did not yield any results.

11. Introduction of transposition systems.

According to a statement by the liaison officer of SIGINT Station 2 with II/353, fairly primitive transpositions made increasingly frequent appearances in army traffic in the spring of 1945. No such observations could be made in the case of the Air Force until the time of the surrender.

In spite of the perfection of SOVIET systems as outlined in the foregoing, the results of cryptographic effort up to the surrender were satisfactory. 70 to 90% of the material (apart from untouched meteorological messages and five-figure adder messages) could be read currently.

In particular, the regional systems of the ground organisation, which were particularly important from an intelligence aspect, could nearly always be broken.

Successes in dealing with the keys of flying units were on the whole less numerous in proportion to the volume of traffic available, but on the other hand the contents of the messages were of lower intelligence value.

IV. THE MODUS OPERANDI OF GAF CRYPTOGRAPHY IN DEALING WITH SOVIET AIR FORCE SYSTEMS.

Preliminary note: An attempt has been made in this section to describe typical features of the cryptographers' modus operandi and of the various stages of their work, and to reduce these as it were to a common denominator. The difficulty of describing a partially creative effort must, however, be obvious.

A. Breaking a new cipher.

These notes are concerned with the handling of SOVIET substitution systems. They can all be dealt with together. Only the modus operandi with adder systems is given a short chapter on its own.

1. Analysis of the message.

Counting the number of cipher groups, determining frequencies and comparing cipher groups in respect of their relative positions in the cipher text are the bases of technical cryptographic analysis.

a. The statistical picture.

The count of the individual cipher elements is made uniform by the introduction of rules which are in general use by all cryptographers. In order to reduce the time taken by this

Doc ID: 6587327

process, a number of different statistical pro formas have been adopted.

b. Normal statistical picture.

The first statistical process applied to a cipher text is unequivocally laid down. The result of this process is in a way the message's "visiting card". The inflexibility of this process proved to be particularly important after the introduction of regional methods, because numerous methods cropped up simultaneously and all of them had practically the same appearance. The number of elements in each cipher group was vital for working out the normal statistical picture.

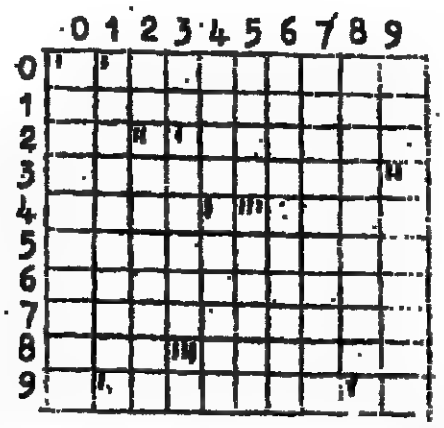
aa. Normal two-figure statistical picture.

The two-figure groups are written in a small 10 x 10 square in which the A-value is read off on the left and the B-value on top. A stroke is made in the intersection square.

Example:

22 45 83 01 45 39 00 22 45 83 44 91 39

83 23 97 etc.



bb. Normal three-figure statistical picture.

For three-figure texts a 10 x 10 sheet of the size of the message form is used. A-values are read off along the top, B-values on the left. The C-value is written in the intersectionsquare. A repetition of a group is noted by a stroke after the C-value.

Example:

439 710 555 386 710 389 411 835 740

989 716 369 002 536 940 537 +

For statistical picture, see page 46

cc. Normal four-figure statistical picture.

The same form is used as that described under para. bb, but in this case A-values are read off on the left and B-values on top. The CD value is treated as one entity and inserted in the appropriate intersection square. If a group is repeated, this is indicated exactly as in the case of a three-figure message.

For statistical picture, see page 47

Doc ID: 6587327

Owing to their unimportance to a fairly large number of workers, no hard and fast rules were established for dealing with five-figure or any letter statistical pictures.

2. Reduction of the normal statistical picture.

The next task is an attempt to reduce the size of the normal statistical picture on the basis of the observations made. This is done by trying to eliminate positions which have obviously been left blank. One "deflates the balloon".

In addition, the statistical picture is as far as possible made to conform to the presumed original, i.e. to the external shape of the cipher basis. This involves eliminating dummies, discovering and assembling values which have been variously reciphered and determining marginal values or "tie-ups" [Nahtstellen] of recognized sector reciphierings.

The nailing down and elimination of any indicators from the cipher text belongs to this process also. Figures in clear in the body of the cipher text also disturb the statistical reciphering picture and must be removed.

Example: see pages 48 and 50

3. Stripping of reciphers.

Since the groups used in a single reciphering are insufficient for a further successful analysis of the method, an attempt is made as early as possible to reduce various encipherments of a method to a common denominator, to collate them and to assimilate them one to another. The most distinctive reciipherment is generally used as a relative basis for this. The easier the reciphering system, the easier the process of assimilation. Measured by the standard systems of the latter years, early assimilations were only very incompletely successful: it was impossible to achieve complete fusion of all reciipherments and partial results had to be accepted, e.g. the correlation of page reciipherments but not of line reciipherments etc.

Errors of varying magnitude cannot always be avoided in the assimilation process. For this reason it is apparent that the cipher groups of different reciipherments can be distinguished one from another in a combined statistical picture, even subsequently, by entering them in different colours.

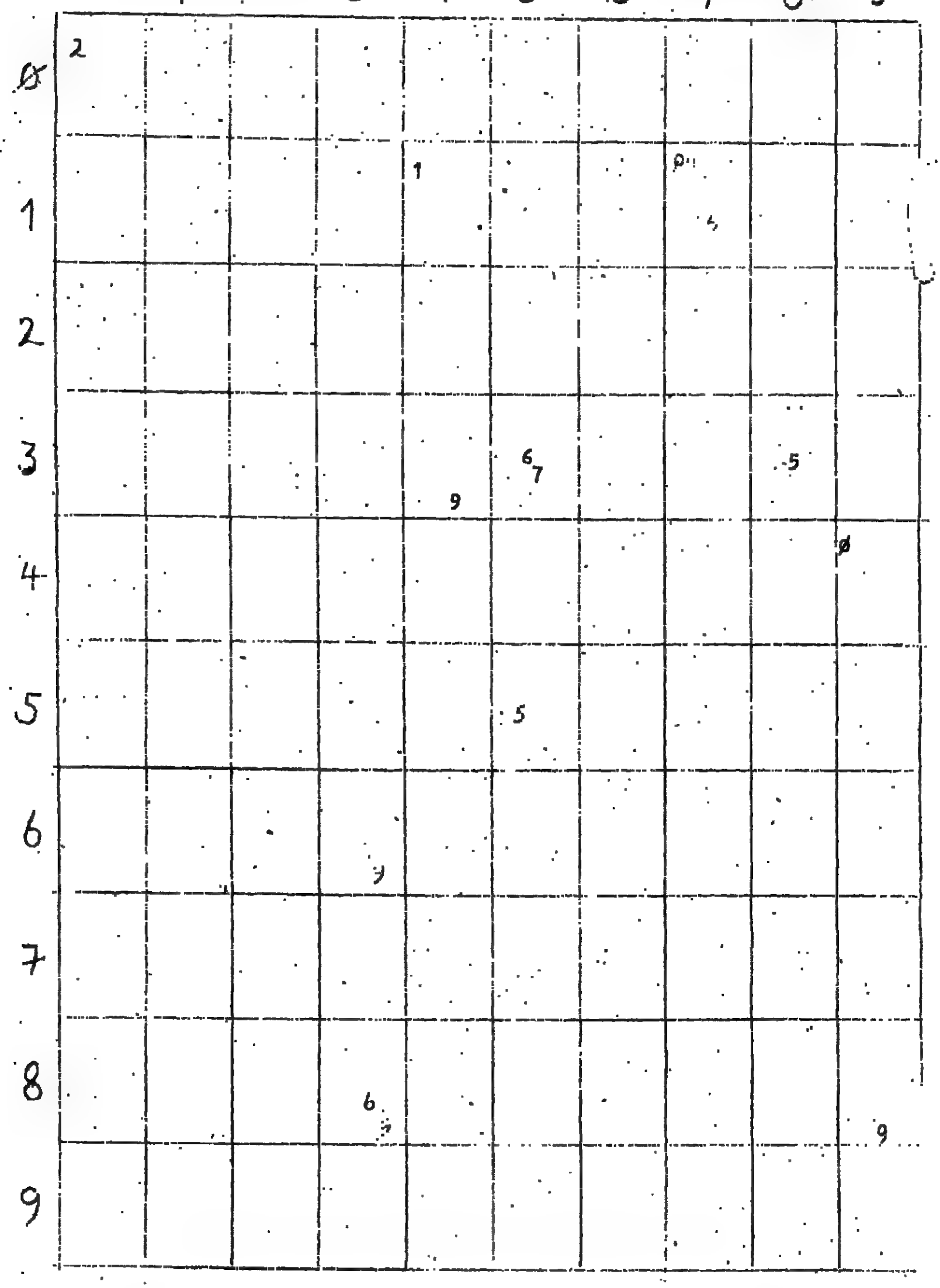
Even when only partial success is achieved in this respect, it is usually possible as a result to recognise the function of the individual values of the indicators. But if these functions are known, then an assimilation of reciipherments with very colourless statistical pictures will also be possible, solely on the basis of the indicator.

Example: see pages 48 and 50

4. Breaking into the system.

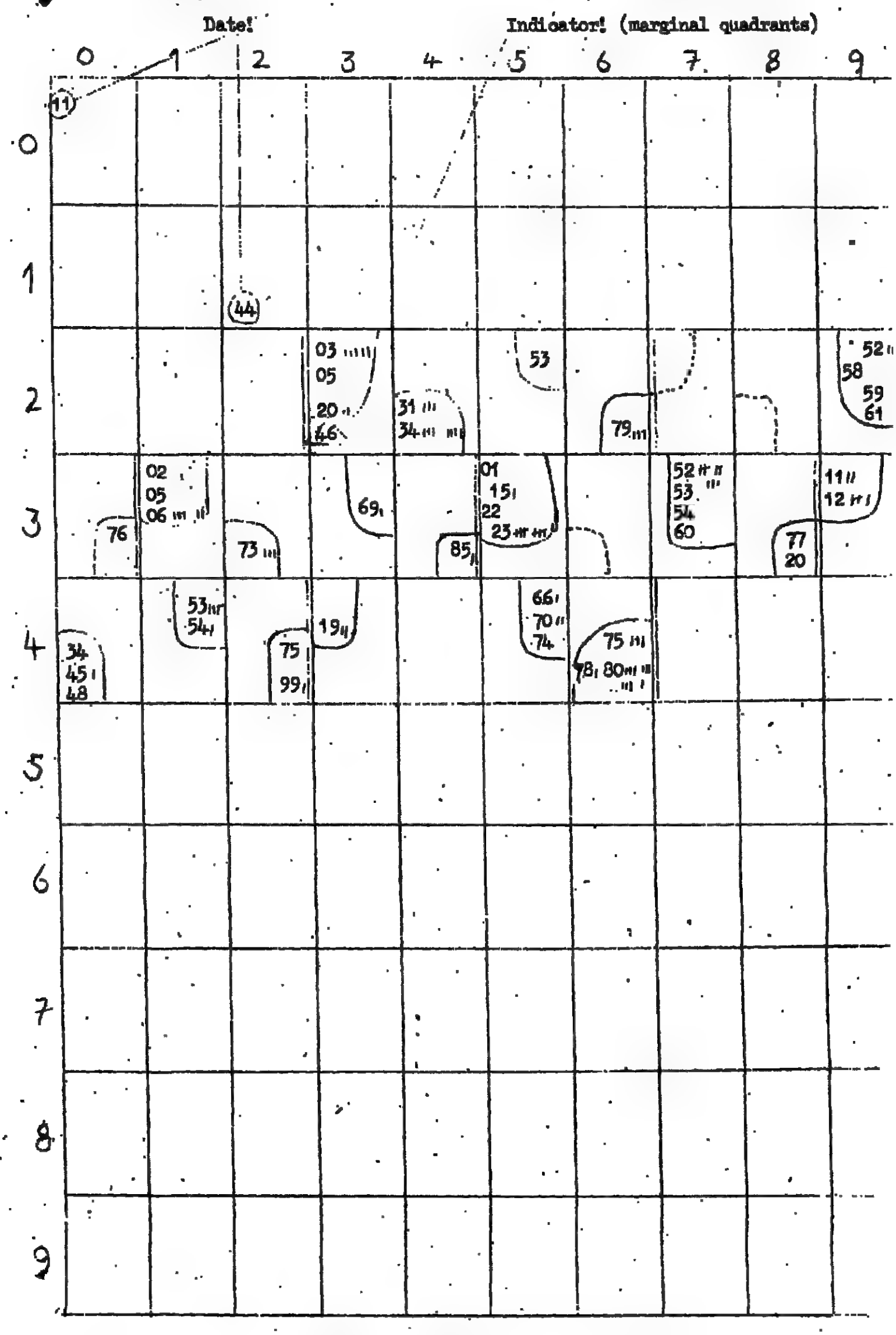
After having carried out the processes described above, a break into the cipher system was often achieved: the cipher material is no longer amorphous, and meaningless but already has

Doc ID: 6587327



Example of a normal three-figure statistical picture.

Doc ID: 6587327



Example of a normal four-figure statistical picture.

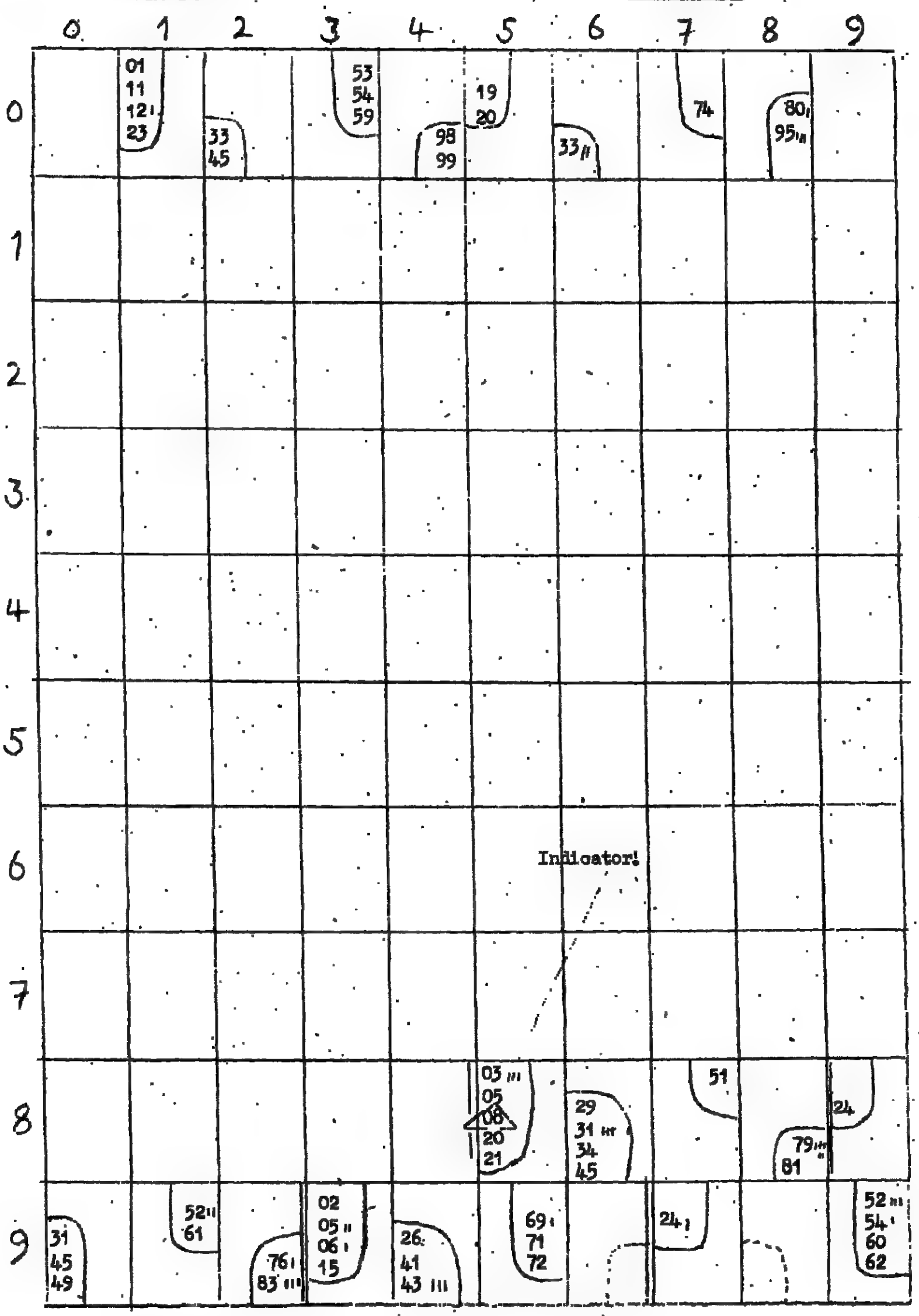
Cipher groups: 2346 3485 2303 3523 4680 etc.

Doc ID: 6587327

23 03 III 01 05 20 II	27	31 02 05 06 III II	35	01 15 I 22 23 III III II	39 11 II 12 III I	43 19	
24 31 III I 34 III III	28	32 43 III	36		40 34 I 45 I 48	44	
25 53	29 52 II 58 59 61	33 69 I	37	52 III III III 53 54 60	41 53 54	45 66 I 70 II 74	
26 79 III	30 76	34 85 I	38	77 90	42 75 I 99 I	46 75 III 78 I 80 III III III	

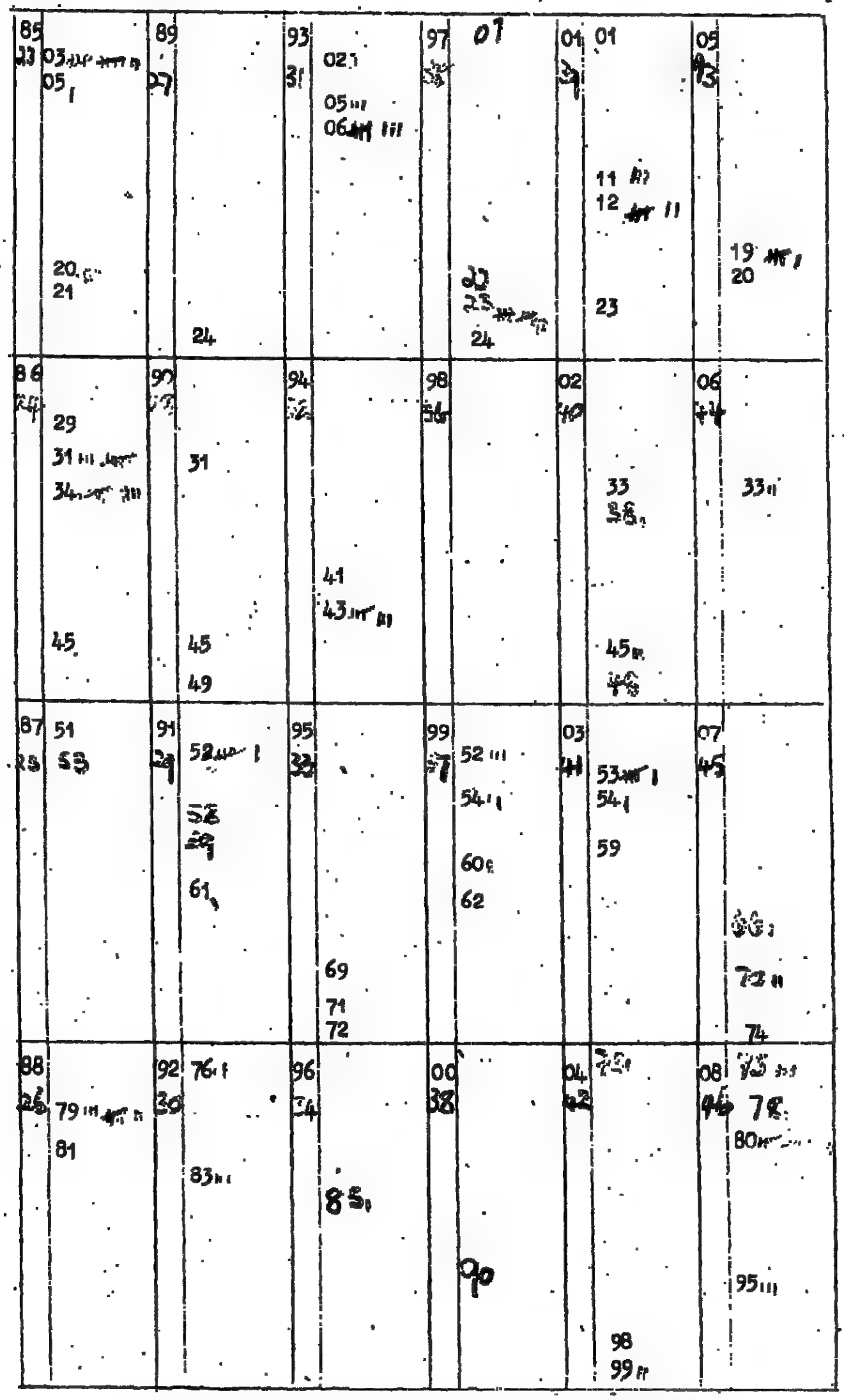
Reduction of the normal statistical picture on page 47

Doc ID: 6587327



The normal statistical picture of a second recipherment (see page 47).

Doc ID: 6587327



Reduction of the normal statistical picture on page 49.
Stripping of the recipherments on pages 47 and 49.

Doc ID: 6587327

a marked individual appearance. Some characteristics of the method can already be enumerated, even though the interpretation of many an observation is still obscure.

5. Breaking into the cipher text.

Now is the time to start trying to break into the cipher text, to read fragments; then the interpretations of the various items must be confirmed in another part of the message and in a different combination.

In the case of code-books having items with two meanings (a letter and a word) it will be necessary to extract certain switch groups and their interpretation and to isolate the pure letter texts. Admittedly, this may be very difficult, especially when the amplifying group in the key data have several meanings and are used completely unsystematically. Sometimes, for instance, very frequently recurring amplifying groups act as very troublesome dummy groups.

6. New interpretation of items, decoding.

Decoding becomes easier in proportion to the progress made in dealing with the method in general. If for example the key basis is only relatively worked out, decoding will of course be more difficult than if the key basis has been reduced to its original values and it is merely a case of systematic reconstruction.

7. Recovery of original basic book.

Even though it becomes possible to read other recipherments also when a relative basis has been recovered, i.e. when a given recipherment has been decided on as interim basis, and even if this offers no great difficulties; recovering the actual original key basis and the reduction to basic values of the relative basis, are matters of the greatest importance; not only because decoding will then be much easier but because only then can different relationships and governing laws in the reciphering system become apparent at all.

Every case of conformity to a law in the construction of the original key basis facilitates its reduction to the latter: in many cases it is this which first makes it possible.

8. Recovering the reciphering system.

The systematic collection of all available reciphering rows with their appropriate indicator values leads to the reconstruction of the entire reciphering system: interesting relationships and laws can be discovered in the course of these efforts.

9 Working out the system.

Repeated work on the material already handled, which is of course still full of incorrect and uninterpreted items, enables one to fill up gaps in the key data and finally to solve all questions regarding the original, the reciphering system etc.

Naturally, the practical pursuit of cryptography often enough led to more or less important departures from the procedure described above. Depending on the characteristics peculiar to a given method, the

Doc ID: 6587327

sequence of theprocesses was altered or else several processes were carried out in parallel and simultaneously; in many cases they were simply omitted.

For the truth of the matter is that the classic and scientific path was in most cases shortened, either by carelessness in enciphering on the enemy's part or by errors and weak spots in the build-up of his cipher methods.

10. Naming the systems which had been solved.

Even before the war, every system dealt with and solved was given a serial number prefixed by the letters "R.O" (Russian Code). As the systems remained in force for a fairly long time, however, their original SOVIET designation occurred in some context or other in the text of a message: this designation was then adopted within the cryptographic organisation.

It had become customary in the general reporting set-up of the Listening Service to refer to systems according to the number of digits in their cipher groups (three-figure code; five-figure adder system etc.). As long as the number of systems in use simultaneously remained small there was no particular objection to this habit, even from the cryptographic point of view. But after the sharp increase in the number of cipher systems in simultaneous use, any division according to the number of digits in the cipher groups became utterly meaningless.

The commonly-held opinion that the security of a system and the importance of the messages enciphered by its means depend on the number of digits in the cipher groups ("The larger the number of digits in the cipher group, the more important the message and the harder it is to decipher") is only very conditionally correct: for the number of digits can be increased by the use of dummies, checking figures and unnecessarily high reciphering figures. Thus an increase in the number of digits does not necessarily indicate an increase in the size of the cipher instructions. But the security of a cipher by no means necessarily increases in proportion to the size of the cipher instructions; on the contrary it can even be diminished. Thus for example a four-figure code book with single reciphering is easier to break than a three-figure table containing, say 200 items, with complicated reciphering and unsystematic construction. In just the same way it has been shown time and again that the intelligence value of a message in no way depends on the degree of security enjoyed by the system chosen for enciphering it. It was for instance noticeable during the first year of the war against the SOVIET UNION that the five-figure messages, reciphered by means of subtractors and used even by higher HQ's, by no means contained the important revelations which had been expected; they were in fact mostly less important than the comparatively simply enciphered messages of any RAB. This caused general disappointment in Intelligence circles.

Every cryptographic department on the Eastern front gave serial numbers to the systems which it had broken, independently of their importance, of the period of their validity or of their traffic density: an additional digit indicated the number of digits in the cipher group.

Doc ID: 6587327

Examples:

Abteilung I: VN (Northern system*) 157/3 - the 157th method to be solved by the Abteilung (three-figure groups).

Abteilung II: VO (Eastern system*, from Wireless Listening Abteilung East) 122/4 - the 122nd method to be solved by the Abteilung (four-figure groups).

Abteilung III: VS (Southern system*) 77/4, etc.

Every method was at once reported by teleprinter or by wireless to the regiment, where it was given the next universally accepted RC number, but only if the method did not seem to be too elementary and if it persisted in use after a few days, since methods often disappeared by reason of the great volume of traffic. Serial numbers reverted to 1 at the beginning of the Eastern Campaign: just before the surrender the 920th RC number was allotted.

B. Breaking the five-figure Adder Systems

As already mentioned, only those adder messages can be broken which have been reciphered by means of the so-called "universal blocknote". Therefore only such messages are dealt with in this chapter.

Breaking these messages depends on the assumption that the difference between two code-book groups equals the difference between these two groups after they have been reciphered with the same adder group.

/ $a - b = (a + w^1) - (b + w^1) = a + w^1 - b - w^1 = a - b$ /

1. Determining the indicators (starting points).

The indicators of an adder table can be found without special difficulty, because at a given place in the message the ABC and the DE values will recur. It is thus possible to work out a system of starting point indicators.

2. Writing messages one below the other.

With this system of indicators the messages can be written one under the other in such a way that the groups in the messages which have been reciphered with the same adder group lie directly one below the other.

3. Compiling the catalogue of differences.

Next, in each column of groups all differences are worked out, and of two possible differences it is agreed that only the lesser shall be valid.

Example:	37529	89553
	-89553	-37529
	58076	52034

TRNS: *German "VERFAHREN NORD, V- OST, V- SUED" respectively.

/ w in this equation presumably for "WURM" = adder.

Doc ID: 6587327

Of the two differences, 52034 is taken because it is the lesser.

These differences are registered in a catalogue, classified both according to frequency of appearance and to the columns from which they are taken: thus every recorded difference out of the available material can at any time be found.

After some time there will accumulate in the catalogue of differences a number of the latter which can be used as standard differences for subsequent stages of the work. According to the laws of probability it can be assumed that identical code-book figures are the basis of equal differences; this assumption will of course entail a whole series of errors which will be recognised and rectified only at a later stage.

4. Relating different columns to each other.

After determining about 10 standard differences, work is carried out only on those columns in the message collations which:

1) have the greatest possible depth, and
2) contain as many as possible of these standard differences.

A particularly favourable column is chosen to be the standard column, i.e. the corresponding adder group is assumed to be zero. If then another column gives the same differences (both minused and subtracted having of course different values), then this column can be equated with the standard column and the relative adder group of this column will be determined.

Example:

Standard column	77777 = relative adder group
a 12345	e 88888-77777 = 11111
b 00000	f 89012-77777 = 12345
c 85665	g 77777-77777 = 00000
d 11111	h 93452-77777 = 26785

a-b=12345 = f-g=12345
d-b=11111 = e-g=11111

a = f
d = e
b = g

12345+77777 = 89012
a f

11111+77777 = 88888
d e

00000+77777 = 77777
b g

After this "assimilation" the groups in the new column can be directly compared with the groups of the standard column, i.e. it is now possible to start drawing up frequency statistics.

Doc ID: 6587327

5. Frequency statistics.

As soon as a column has been assimilated to the standard column, the newly calculated groups (cipher group - identified adder group) can be included in simple frequency statistics : at last, one can reckon in terms of comparable sizes.

6. Decoding.

If fairly large complexes of columns have been assimilated, a start can be made with the interpretation of the groups: the first item interpretations, that is, the first breaks into the text of the message are achieved.

7. Recovery of original cipher instructions.

This process consists merely in discovering the true adder group of the standard column. Given non-hatted construction of the code-book, this stage of the work can be carried out promptly. When dealing with the five-figure code-book during the year 1939, figure enciphering used in this method was successfully employed to reconstruct the original data. As a matter of fact, figures were reciphered only with the appropriate adder group; the correct date, time and unit figures were easily found.

C. Deciphering.

When a system had been solved, its messages could be read currently by the shift service of the appropriate deciphering department.

1. Cipher recognition service.

The multiplicity of systems which were simultaneously in force made it necessary to identify the material.

a. Call-sign or network identification.

If the network on which the messages had been transmitted was already known, such messages were sorted out and given some call-sign identifications before being deciphered. If call-signs had been identified, the appropriate system could be determined without difficulty.

If, however, no information was provided by traffic analysis, then identification had to be done by the deciphering section without outside help.

b. Code (SIGNAL) groups.

Some of the systems were indicated by a special code group in the text: such a group had to be particularly obvious. Doublets etc. were much favoured (e.g. 5555, 777 etc.). Sometimes the code was given as a word (e.g. "oka", "rubin" etc.). Difficulties in identification occurred only when by chance the same group was used in different sectors of the front for different systems: this was a not infrequent occurrence. In such cases D/F aids were valuable.

Doc ID: 6587327

c. Key groups (indicators)

Since cipher texts without indicators were the exception, especially in recent times, indicators could only exceptionally be used for identification purposes - and then they had to be very clearly differentiated.

d. Address groups

Enciphered address groups were as a rule identical throughout the Air Army: hence they could only comparatively rarely be used for unequivocal identifications.

Clear text addresses (surnames and, less often, military units) could be used for identification by referring to special indexes.

e. General message characteristics.

Sometimes peculiarities (such as interpolated clear text, date groups at the end of the message, unusual preambles etc.) led to workable identifications. But even these observations were not always unambiguous.

f. Statistical picture.

Sometimes it was possible to recognise the system at a glance from the statistical picture. Since, however, the statistical pictures were not in most cases greatly differentiated owing to the choice of reciphering systems, successful identifications of the system used became even rarer by this means, which in any case required the use of trained and adaptable personnel.

2. Recipher investigations.

Even in the case of known systems, the recovery of new reciphernents gave a certain amount of trouble.

Apart from peculiarities of a stotistical nature, the building up of new reciphernents was facilitated by a number of circumstances.

a. Contents of the message.

In fact, the building up of a new reciphernent was very considerably assisted by the regular transmission of stereotyped or at least similar messages. Thus, for example, a daily airfield serviceability report enables one very easily to reconstruct new reciphernents.

Even the presence of an identified address group enables one to draw conclusions as to the actual text (e.g. "to the divisional M.O.").

The repetition of an order by STALIN, for example, repeated on many different wireless networks with but few minor variations, may be recalled: this enabled reciphernents of numerous systems to be recovered in parallel. On special holidays (e.g. RED ARMY day etc.) almost identical congratulatory addresses were transmitted and these coloured all the work on a particular day, and also simplified it.

Doc ID: 6587327

b. The reciphering system.

When the reciphering system is known, new reciphernents can also be recovered with comparative ease. When systematic rows or distinctive habits are in use for reciphering, often only a single clue is required for one to be able to build up the entire reciphernent.

c. The basic code.

Every peculiarity or system of the basic code can similarly yield the required clue for recovering a new reciphernent.

3. Interpretation of new items.

Successful decoding postulates good linguistic knowledge. In addition to this a certain knowledge of tactical procedure is necessary.

Efforts were variously made to compile an extract of the SOVIET vocabulary from the numerous recovered cipher instructions, the few captured instructions and the broken material available. The "universal code-books" recovered by this method have time and again rendered valuable services in decoding.

D. Aids to Cryptography.

1. General aids and data.

Just as cryptography is an auxiliary service for other departments in the general set-up of the Listening Service, so too are all the results achieved by other departments auxiliaries to cryptography.

All traffic analysis and D/F data (call-sign identification, network, diagrams, D/F results) and content and final evaluations (composite reports, dispersal tables and maps, unit and personnel indexes, lists of abbreviations, type designations and military dictionaries) are continually of assistance to cryptography. Continuous liaison with the different specialists is of the greatest possible value.

2. Special aids and data.

a. The statistics proformas.

Various proformas were available for the numerous statistical researches; they were at the same time used for reconstructing cipher instructions. The cryptographer was able to cope with all necessary tasks with the help of such proformas and did not need to waste precious time in making them up by hand. Only in the rarest cases did the draughtsmen of the evaluation department have to make special designs themselves. This fact was particularly advantageous in view of the primitive conditions in the East.

b. Language statistics.

Letter and bigram statistics etc. of the RUSSIAN language were available from pre-war days, but they were used neither for new key breaking nor for current work. The few basic rules (frequency of letters) which could be used and which were of importance for every cryptographer were easily memorized by everyone.

Doc ID: 6587327

c. Special Indexes.

Special indexes were provided in particular for the cipher identification service: they were adapted to current needs at relatively short intervals. Proper names, message peculiarities, statistical pictures, characteristics of the different systems, code groups, etc. were indexed currently and continually brought up to date.

d. Message files.

All broken messages were returned after intelligencing to cryptography and sorted out according to system (i.e. at the same time according to network) and kept for a few months before being sent on to the CHI-STELLE. These message files proved very valuable when working out new systems and for the training of fresh personnel.

V. EXAMPLES OF SOVIET AIR FORCE CIPHER SYSTEMS IN USE DURING THE CAMPAIGN IN THE EAST.

The author has attempted to portray in a few examples the typical features of SOVIET systems. These examples are more or less arbitrary constructions, since his powers of memory obviously cannot stretch to a complete reconstruction of systems actually in use. On the other hand a particular system has been borne in mind which while framing every one of the examples: lapses of memory have been filled in arbitrarily, but still by means of frequently recurring typical instances.

1. The examples on the following page illustrate two aspects of the reconstruction of PT-tables (general cipher systems in use by wireless operators at their transmitters) in the years 1939 and 1942.

The upper table is a reconstruction of PT-39. The alphabet with single meanings is built up systematically: the system is indicated by the yellow lines. The blue dashes in the various squares indicate individual and sentence items: the vocabulary is to some extent comparable with that of the international Q-code groups. The reciphering figures along the margins are taken from the system table on page 24.

The lower table is a PT-table of 1942 (PT-42-1). Incidentally, four different tables were used simultaneously in 1941 or 1942. The alphabet has two meanings, only one of which is arranged systematically (yellow lines). The reciphering rows along the margins are also taken from the system table on page 24.

Doc ID. 6587327

	8	1	3	6	9	2	7	4	0	5
8				а	к	ф	я	9		
7				б	л	х	о	⊙		
1				в	м	ц	1	(ı)		
4				г	н	ч	2	(–)		
5				д	о	ш	3	(:)		
9				е	п	щ	4	(δ)		
6				ж	р	ь	5			
3			(c)	з	с	ы	6			
0				и	т	)	7			
2				й	у	ю	8			

	5	3	7	2	4	1	6	9	8	0
4	а		л		ø		5	к	т	ф
6	х	б		в	ц	7	б	ю	у	7
2	)	ц	в		з	е		т	6	2
5	х	о	ч	г	и	щ	с	5	н	⊙
3		1	а	щ	д	р	ч	р	ь	9
8	г	м		ф	п	е		д	(–)	у
1		6		о	з	щ	ж	п	ч	(c)
0	8	ч	н	2	ц	з	ь	з	с	ы
7	(ı)	м	1	ю	ч	⊙	(ı)	ы	и	(δ)
9	л	ø	ре	(–)	(:)	н°	(?)	о	)	к

Doc ID: 6587327

2. Key tables with 200 positions.

The basis of this reconstruction is the method in use by the 56th RAB (at the beginning of 1945).

The cipher instructions consist of two pages, each with 2 x 5 quadrants with 10 items each. The items are only partially alphabetically arranged, the figures 0 - 9 unsystematically arranged. Two switch groups allow of using the whole item on the initial letters only.

Reciphering is done by means of two strips. Each reciphering strip is indicated in sectors by a two-figure group.

For a period of one month, 10 strips with different indicators from 00-49 and AB-values (quadrants) from 50-99 (also in sectors) and 10 further strips with indicators from 50-99 and AB-values from 00-49 are issued. Two strips from each of the strip series can be combined for each recipherment.

Example of a cipher message. The reciphering strips are placed alongside the data on page 61

2555	(Indicator)	855	4
024	ⓞ	881	ⓑ
001	naö	748	a
016	chtaba	152	p
896	diwizii	024	ⓞ
106	ⓞ	017	na
152	prochu	015	nach
988	soobqitx	748	a-rodrom
759	kogda	146	ⓞ
811	ⓑ	487	major
988	s	841	ⓑ
699	ä	210	p
896	d	098	o
668	e	152	p
523	t	357	o
014	ⓞ	710	w
705	1	116	ⓞ +
325	7		

Criticism of the system.

In spite of the small number of items, cipher security is fairly high, especially when letters are correctly enciphered so that no frequency peaks appear in the message statistics. In the case of individual reciphering of the C-values (lines) reconstruction of the actual original data is very difficult because the significations are not arranged alphabetically according to their initial letters and are spread over various quadrants. The indicators are easily recognizable if only because they have a different number of symbols. It is comparatively easy to collect different messages having the same recipherment because the sector values of the indicators are easily found on account of the switch groups in the code-book, these having but one meaning.

	24-31						50-57				
а....	5			2	В....	л....	9			9	О....
а....	8			4	В....	л....	3			0	О....
а....	9	61	70	5	1	л....	8	Ø3	35	6	О....
а....	2			0	В....	л....	6			1	О....
а....	4	|	|	6	В....	л....	4	|	|	7	О....
а....	3	65	73	7	С....	л....	5	Ø8	37	2	О....
а....	1			9	С....	л....	1			4	О....
0	6			3	С....	ц....	2			5	П....
а....	0			8	Т....	ы....	0			3	П....
а....	7			1	Т....	ь....	7			8	П....
а....	2			6	Г....	л....	9			7	О....
а....	3			1	Г....	7	5			1	О....
а....	4			7	Г....	л....	2			6	О....
а....	7	94	50	0	С....	л....	6	3Ø	15	4	О.... 6
К....	9	|	|	5	С....	л....	3	|	|	9	
К....	0	96	54	2	Т....	л....	0	34	21	8	О....
К....	6			3	Т....	ц....	4			0	П....
Р....	8			4	Т....	ц....	8			5	П....
Р....	1			9	Ч....	8	1			2	
Р....	5			8	Ч....	л....	7			3	П....
а....	3			1	д....	М....	3			5	О....
а....	7			6	див	М адор	9			2	О....
аэродром	8			3	д....	М	7	43	Ø9	8	О....
К....	0	74	89	4	д....	М....	8			0	О....
Когда	9	|	|	5	Ф....	л....	6	|	|	4	О....
К....	1	80	93	7	Ф....	л....	4	49	14	6	0
Р....	5			9	Х....	л....	2			3	П....
Р....	2			8	Х....	л....	1			7	П....
Р....	4			0	Э....	л....	5			1	П....
Р....	6			2	Ю....	щ....	0			9	П....
б....	0			7	Е....	Н а	7			5	О....
д....	1			8	Е....	Н ак	1			2	О....
б....	6			5	Ж....	(С)	4			0	П....
2	3	97	66	2	Ж....	Н аш	5	ØØ	26	7	П....
Р....	9	|	|	4	З....	Н....	2	|	|	4	П....
Р....	2	99	69	3	З....	Н....	3	Ø2	29	6	П....
С....	4			0	З....	Ш....	0			8	П....
С....	7			6	Ф....	Ш....	9			9	П....
С....	5			1	Х....	Ш таб	6			1	П....
Сообщить	8			9	Ч....	Ш....	8			3	9
б....	9			5	4	Н....	6			4	О....
б....	5			2	Ц....	Н....	3			5	О....
С....	4			7	Ц....	Н....	7	22	38	7	О....
С....	2	55	81	1	(б)	Н....	5			0	П....
3	3	|	|	0	Ц....	Н....	4	|	|	2	П....
С....	1	60	88	3	Х....	О....	9	25	42	3	П....
С....	7			9	Х....	О....	1			9	П....
Т....	8			4	(—)	5	2			8	П....
Т....	0			8	Щ....	О....	8			1	П....
Т....	6			6	Ч....	О....	0			6	П....

Doc ID: 6587327

3. Cipher table of a flying unit.

This is a reconstruction of a table of VIII CHAK.

The basic key consists of 9 columns, each with 9 quadrants of 9 lines each. Only the lines are numbered right through (1-9) in the original. Every line is divided into two portions; the left-hand portions contain letters and the letters within a quadrant - read from top to bottom - build a word; the right-hand portions of the lines are filled with completely unsystematically arranged word items and with figures. The choice of the required halves of lines is regulated by switch groups (having only one meaning).

Reciphering. The table is reciphered by means of two 9-symbol rows of figures with single-digit individual numbers. The lines remain constant. In the reciphering rows used, the values 0 are in all cases lacking, so that the message statistics are strongly differentiated in consequence. No indicators are used but their place is taken by the switch group. The first group of the message is in every case one of the two switch groups: the AB-values which are the same in both switch groups may therefore be reckoned as indicators. No system in connection with the reciphering rows could be determined.

Example of a cipher message. In the reconstruction of the key on page 63 only the 4 top quadrant lines are shown in part: the lower 5 are missing. The red reciphering figures are arbitrarily placed alongside.

833 (ä) , the AB-value, simultaneously indicator.
476 n
675 e
753 m
474 e
175 d
155 l
156 e
777 n
759 n
973 o
836 (g)
759 donesti
152 mesto
833 (ä)
476 n
159 a
733 h
734 o
735 v
175 d
372 e
879 n
631 i
638 ä +

Criticism of the system. The cipher security of the table is fairly high because all letters have more than one meaning and if the letter items are cleverly chosen no agglomerations will occur. The completely unsystematic arrangement of the word items does, however, tempt the encipherers to encipher almost exclusively letters for the sake of convenience. - It is very difficult to recover the basic key: word meanings of the letters in a quadrant become apparent only after fairly lengthy work. The fact that the C-values remain constant does, however, ease the task. The switch groups which have only one meaning enable one to distinguish without difficulty between letter and word portions within the cipher messages.

Doc ID. 6587327

		7		6		1		4		5		8		9		2		3
5	1	Н	ПРОШУ	П	И...	С	Ч....	А										
	2	Е	ЛИМИТ	Р	Л....	А	??	Э										
	3	М	ДАТЬ	О	Р....	М	МЕСТО	Р										
	4	Е	ПОЧЕМУ	Ш	Н....	О	Ь....	О										
	5	Д	НАЧ	У	Д....	Л	И....	Д										
	6	Л	НА	В	С....	Е	Т....	Р										
	7	Е	ЭШЕЛОН	Ы	К....	Т	П....	О										
	8	Н	ДЛЯ	С	У....	Н	??	М										
	9	Н	ДОНЕСТИ	Л	В....	А	Р....											
7	1	В		Ю		З		С		Ю		Ю		Ю		С		С
	2	О		Ж		А		Е		Г		Г		Г		Е		Е
	3	С		Н		П		В		О		О		О		В		В
	4	Т		е		А		Е		В		З		В		Е		Е
	5	О		е		Д		Р		О		А		О		Р		Р
	6	Ч				Н		Н		С		П		С		О		О
	7	Н				Е		Е		Т		А		Т		З		В
	8	Е				Е		Е		О		Д		О		А		О
	9	Е								Ч		Н		Ч		П		С
3	1	Н		И														
	2	А		С														
	3	Х		Х								Л						
	4	О		О														
	5	Ж		Д														
	6	У		Д								П						
	7	С		Н														
	8	Ь		Я														
	9																	
2	1																	
	2																	
	3																	
	4																	
	5																	
	etc.																	

- 63 -

TICOM/I-120

Doc ID: 6587327

4. 10-page code-book of the ground organisation.

The cipher instructions are made up of 10 pages, every one having 10 x 10 items. Conditionally alphabetical sequence: the word groups are arranged according to their initial letters, but the word elements among one another are not arranged with reference to their initials. The figures 0-9 are arbitrarily spread over the pages. Amplifying groups have 10 meanings: every page has a pair of amplifying groups.

Reciphering. The 10 code-book pages (A-values) are reciphered with two-digit sector values (AB of the cipher groups). The corresponding reciphering rows are designated in sectors by two-digit identification numbers, but the B-values of the identification numbers are in fact only dummies and can be eliminated without affecting the issue. The 10 page-reciphering rows are changed monthly.

UNCODE

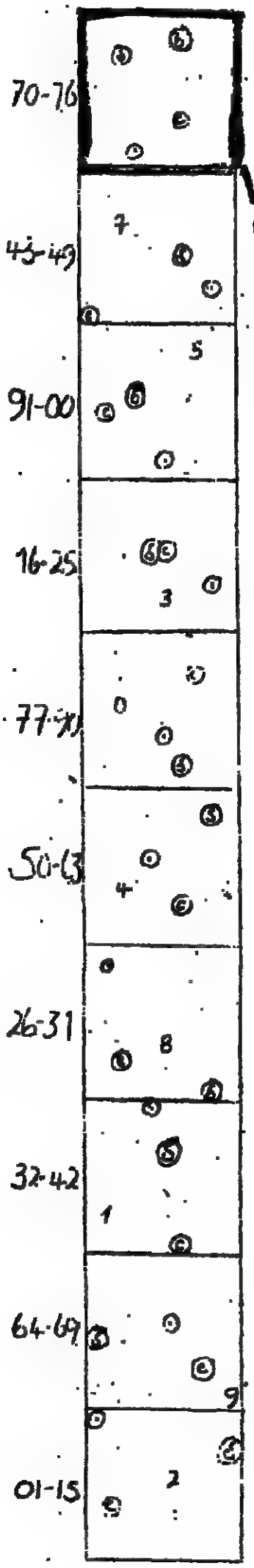
The columns within the pages are reciphered by means of single-digit figure rows. Here too 10 unrelated rows are used every month.

During the course of any given month, the lines (D) are altered merely by means of a row: this row can, however, be varied (drum). The D-value of the message indicator gives the starting point for this line reciphering row.

The reciphering rows of the indicator 5309 are placed alongside the cipher instructions on page 65. The signification "a w ie" for instance, would thus be rendered "7348".

Criticism of the system. The conditionally alphabetical build-up of the data facilitates its reduction to original values (arrangement of pages and columns). The lines, however, could not be re-arranged unless they had been reciphered by means of drum variants. The fact that change-over groups have 10 meanings makes it difficult to differentiate between letter text and word text.

Doc ID: 6587327



	0	4	6	7	8	5	1	3	2	9
6	АЛ	АД	АС	БАТ	БЕР	ВИ	ВАК	ГИ	ДЛЯ	До-клад
2	Аэро-дром	АФ	Авто-бенз.	БЕ	Б	ВЕ	(6)	ГАС	ДА	ЕЩЕ
3	АВТОЛ	АМ	(Б)	БЕС	БО	ВЧ	ВИР	ГА	До-нести	ЕЙ
8	АБ	АВИА	Аппа-рат	БАЗА	БА	ВИН	ВАН	год	ДИ	Е
0	АТ	АП	Авто-машин	БЕЛ	ВО	вечер	В	годен	ДО	ЕСЛИ
5	А	Авиа-ция	АЭ	БАО	ВАТ	вес, в	ГЕ	ГУ	Дайте	ЕН
4	АХ	Авиация в-ка	АЧ	Бата-рея	ветер	ВАР	(С)	ГАЗ	Д	Ежедневно
9	Авиа-бензин	АТЬ	БИ	БЕТ	ВУ	ВА	Г	гаран-тия	Директива	ЕСТЬ
1	АЮ	Акку-мулятор	БЕЗ	(⊙)	ВАС	ВАЛ	ГО	Гаран-тиров	Давать	ЕН
7	Апрель	АВ	Без измен.	БУ	ВАМ	волна	город	Дать	ДЕ	ЕЕ

AB (page)

00-09	10-19	20-29	30-39	40-49	50-59	60-69	70-79	80-89	90-99
22-25	26-32	56-63	07-15	36-44	70-76	08-19	32-45	64-77	50-54
43-55	33-45	20-35	51-69	64-77	43-49	50-65	76-83	82-94	67-73
86-10	78-86	08-19	96-06	13-21	91-00	79-91	17-25	17-21	95-01
60-72	54-69	91-99	23-33	03-12	16-25	45-49	46-53	22-36	02-11
26-32	93-01	74-76	70-76	60-63	77-90	20-35	84-97	05-16	55-66
80-85	02-11	43-55	42-50	93-02	50-63	66-71	26-31	71-81	86-94
11-21	70-77	00-07	16-22	78-81	26-31	92-99	98-08	45-49	26-31
56-59	87-92	77-90	90-95	22-35	22-42	00-07	54-60	50-63	12-25
73-79	12-25	36-42	77-89	82-92	64-69	72-78	09-16	95-04	32-49
33-42	46-53	64-73	34-41	45-59	01-15	36-44	61-75	37-44	74-85

C (column = quadrant)

	0	4	6	7	8	5	1	3	2	9
0	0	4	6	7	8	5	1	3	2	9
1	8	6	4	0	9	7	1	3	5	2
2	8	1	9	4	2	0	3	7	5	6
3	6	3	7	1	5	0	4	8	2	9
4	3	8	1	7	5	9	4	6	2	0
5	7	1	4	5	6	3	2	8	0	9
6	9	3	5	7	0	1	2	6	4	8
7	9	8	6	5	1	2	4	3	7	0
8	8	6	9	4	3	2	5	1	7	0
9	3	1	0	5	8	6	4	7	2	9

D (line)

0	2
1	3
2	8
3	0
4	5
5	4
6	9
7	1
8	7
9	6

e.g. 5309

Doc ID: 6587327

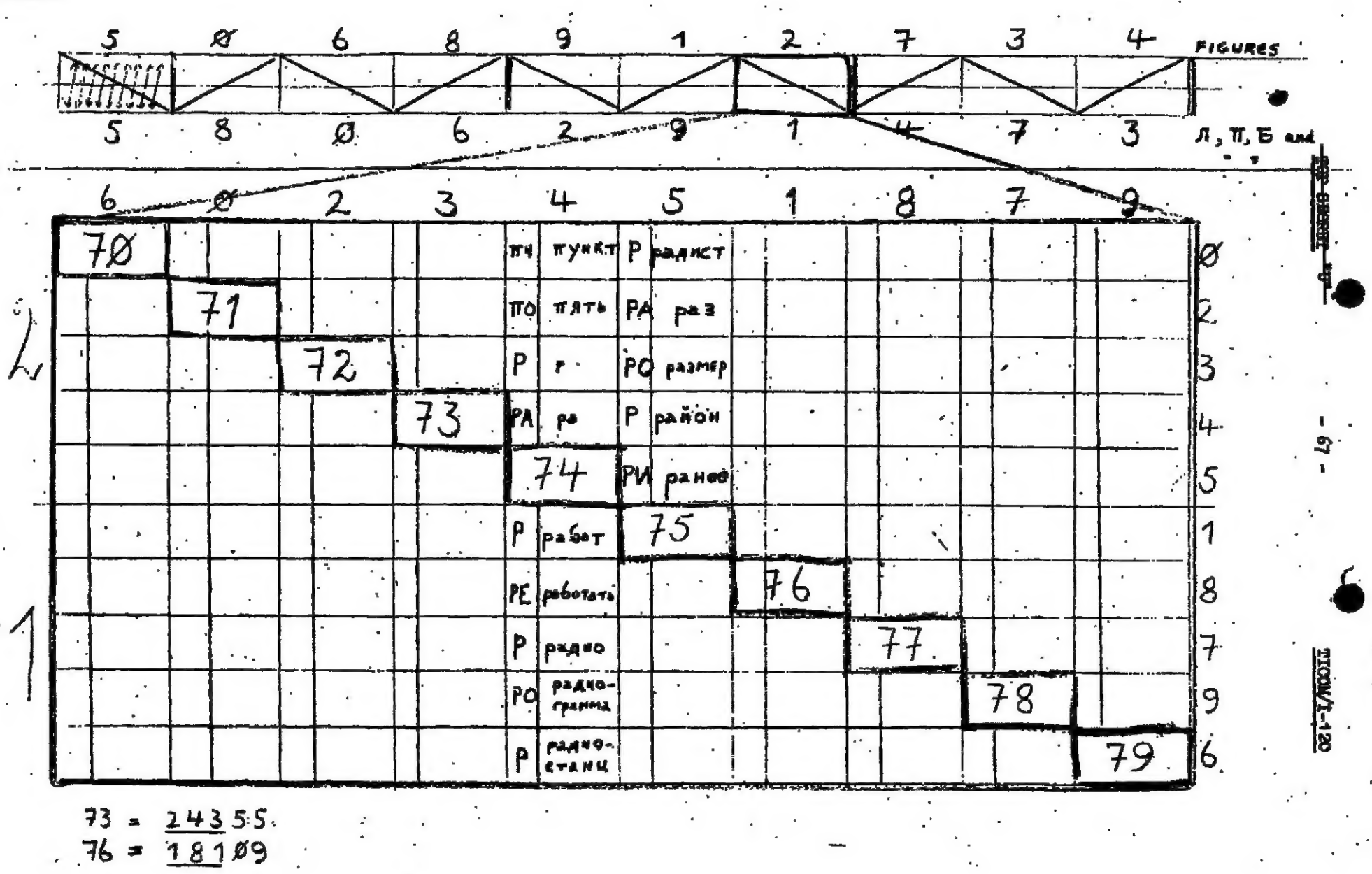
5. 10-page code-book of the ground organisation.

The cipher instructions are built up completely systematically: lexicographic arrangement of words and word elements, systematic arrangement of the numbers 00-99, switch groups in the last column of the last page (with one meaning). The lines are divided: letters and bigrams on the left, syllabus and words as a rule on the right. All items on one line have the same initial letter. While the meanings on the right are built up entirely lexicographically, the bigrams on the left side are occasionally hatted.

Reciphering. The reciphering rows for page and line are coupled together, thus they cannot arbitrarily be varied in respect of each other. The reciphering row for column (B) is a cyclic variant of the corresponding C-row. Method of reading the cipher group: ACBZZ. Two dummies are attached to the original cipher group ACB. Method of reading the indicator at the beginning of the message is also ACBZZ.

Criticism of the system. The systematic build-up of the cipher instructions considerably facilitates all technical breaking processes. Only the hatting of the bigrams on the left side of the columns leads one astray, particularly at first. The switch groups "left", "right" and in addition "letter" also cause difficulties. - The reciphering rows of the month are often simply enough cyclic variants with small variations (transposition of two figure values) and allow one partially to reconstruct unidentified rows. The attaching of the two dummy values to the cipher group is easy to recognise and to eliminate on the basis of the statistical picture.

Doc ID: 6587327



73 = 24355
76 = 18109

TOP SECRET

TICOM/I-120

Doc ID: 6587327

A (page)

6	9	7	8	1	5	4	3	2	0
5	0	8	6	9	2	1	7	4	3
9	2	1	7	4	3	0	5	8	6
1	7	4	3	5	0	6	8	9	2
2	9	1	4	6	0	8	5	7	3
3	7	5	8	0	6	4	1	9	2
0	6	4	1	9	2	3	7	5	8
6	4	1	9	2	3	7	5	8	0
2	3	7	5	8	0	6	4	1	9
9	2	3	7	5	0	8	6	4	1

C (line) + B (column = / quadrant) = drum variant of C

0	3	4	7	1	2	9	6	8	0	5
1	0	2	3	4	5	1	8	7	9	6
2	2	3	4	5	1	8	7	9	0	6
3	0	5	3	4	7	1	2	9	6	8
4	3	4	5	1	8	7	9	0	6	2
5	8	5	7	3	2	9	1	4	6	0
6	1	4	6	8	0	5	7	3	2	9
7	5	0	8	6	4	1	9	2	3	7
8	7	5	0	8	6	4	1	9	2	3
9	6	4	1	9	2	3	7	5	0	8

17655 =
A 5 0 8 6 9 2 1 7 4 3
C 0 2 3 4 5 1 8 7 9 6
B 6 0 2 3 4 5 1 8 7 9

Doc ID: 6587327

Appendix

1. Organisation of Chi-Stelle East.

In practice the two Eastern Sections of the Chi-Stelle (D/Evaluation, E 1/cryptography) were merged into evaluation or cryptographic parties with Regiments; the leading spirit in the Eastern organisation, Major Kupffer became liaison officer at Luftwaffe HQ. Only 2 members of the Chi-Stelle remained with the regiment, Lt. Wisnikow (evaluation) and Lt. v. Lingen (cryptography); however their influence on the organisation of work in the east was very small, all the more because they had been refused both by the Regiment as also by the detachments for technical and also personal reasons.

2. Principles of the SOVIET call-sign system.

Although the author did at one time take a personal interest in this question, he is unable to supply any information on the matter. He remembers only that until 1944, there existed certain relationships between change of call-sign and FT-table reciphering (the reciphering rows were the same for both provinces). It was also possible to establish a relationship between change of call-sign and the reciphering rows of some RAB systems (three-figure). It should, however, be noted that the investigation of the principles underlying the call-sign system was very much less to the fore in the case of the GAF than in that of the Army, because:

1. The smaller number of air force networks allowed from the first of better coverage, even when the daily changes of call-sign took place apparently entirely unsystematically, and
2. because of lack of personnel.

The specialist on the principles of the call-sign system in II/353 was FW. HEINS, a conscientious and successful worker, who is probably at present in HAMBURG, address not known. But in any case the corresponding workers of the Army SIGINT stations will be in a position to furnish better information.

3. The Forschungsamt.

The author knows no details about the work of the Forschungsamt, as its activity was kept very secret. In any case work was done there on diplomatic traffics, at least, however, it was intercepted. Also there was some talk of economic espionage. The staff, were extremely well paid, but were very reticent; the author knew no-one in the Forschungsamt personally.

Neither was it known who was behind this organisation; opinions varied between the Reichsmarschall or the SS (or both). In Riga in 1942 the author received an offer of transfer to the SS (?) cryptographic department from an SS-Führer known to him, who, however, had not been told by him about the nature of his work. Perhaps the Forschungsamt was meant. The head of the cryptographic section was said to have been a former naval officer.